The relationship between the mandatory reporting obligations of NIS2 and GDPR in light of premature public disclosure

LLM Law and Technology

Tilburg University

Tilburg Institute for Law, Technology, and Society

Author: Lisa Beatrice Ferrari

SNR: 2069833

Date: August 2023

Supervisors: Dr Irene Kamara and Manos Roussos

Acknowledgements

I would like to express my sincere gratitude to my first supervisor, Dr Irene Kamara, for her guidance, insightful recommendations, and continuous support throughout the research process.

I would also like to thank my second reader, Manos Roussos, for his constructive feedback, and the time he dedicated to reviewing my work.

Finally, a special thanks to my family, who has been a steady compass throughout this journey.

TABLE OF CONTENTS

Abbreviations

BITKOM	Digital Industry Association Germany
NIS Cooperation Group	Network and Information Systems Cooperation Group
CSIRTs	Computer Security Incident Response Team(s)
DBNO	Data Breach Notification Obligation
DPA	Data Protection Authority
DSPs	Digital Service Providers
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisors
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technologies
ISAC(s)	Information Sharing and Analysis Centre(s)
MS	Member States
NCSC(-NL)	National Cyber Security Centre (of the Netherlands)
NIS	Network and Information Security
NIS1	Directive concerning measures for a high common level of security of network and information systems across the Union
NIS2	Directive on measures for a high common level of cybersecurity across the Union
NIST	National Institute of Standards and Technology -
OES	Operators of Essential Services
SME	Small and Medium Size Enterprise
WP29	Article 29 Working Party

Chapter 1 – Introduction

1.1. Setting the Background: the Problem Statement and the Literature Review

In 2016, the European Union took legislative action by introducing the Network and Information Security Directive, onwards referred to as NIS1, which aimed at achieving a high common level of cybersecurity across the Member States.[1] Around the same period, the General Data Protection Regulation (GDPR) was also enacted, laying a comprehensive legislative framework for data protection.[2] While the NIS1 improved national cybersecurity frameworks, its implementation was proven difficult, leading to fragmentation.[3] Notable shortcomings included the unclear scope of NIS1, as well as the incident reporting obligations and ineffective enforcement.[4] Member States were afforded substantial discretion in implementing these elements, which ultimately resulted in NIS1 falling short of achieving the envisioned harmonization in the internal market.[5] This led to a legislative process which resulted in the adoption on December 2022 of NIS2, the Directive on measures for a high common level of cybersecurity across the Union, on December 2022.[6] NIS2 will enter into force on 18 October 2024, after transposition under the Member States' domestic legal systems.[7] NIS2 broadens its scope of application to encompass a greater number of essential and important entities operating across various sectors.[8] Its three key objectives include the enhancement of cyber-resilience among relevant businesses operating in the EU, the reduction

[1] Maria del Mar and Achiaga Negreiro, 'The NIS2 Directive - A high common level of cybersecurity in the EU' (2022) European Parliamentary Research Service, <https://www.europarl.europa.eu/thinktank/nl/document/EPRS_BRI(2021)689333> accessed 20 August 2023, 2

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC [2016] OJ L 119/1

[3] European Commission, 'Impact Assessment Report accompanying the document 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' (*European Commission, 16 December 2020)* SWD 345 final, part 1/3 *https://ec.europa.eu/newsroom/dae/redirection/document/72176* accessed 20 August 2023, 13-15

[4] Ibid 14

[5] Maria del Mar and Achiaga Negreiro, 'The NIS2 Directive - A high common level of cybersecurity in the EU' (2022) European Parliamentary Research Service, <https://www.europarl.europa.eu/thinktank/nl/document/EPRS_BRI(2021)689333> last accessed 14 October 2023, 2-3

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80

[7] Ibid Article 41

[8] Niels Vandezande, 'Cybsersecurity in the EU: how the NIS2-Directive stacks up against its predecessor' (KU Leuven - Centre for IT & IP Law, 2023) https://ssrn.com/abstract=4383118 last accessed 10 August 2023, 5-6

of overall inconsistencies in cyber-resilience across the internal market, and the improvement of joint situational awareness and overall preparation and response mechanisms.[9]

This research primarily discusses and compares the mandatory reporting obligations under NIS2 Article 23 and GDPR Articles 33-34, intending to investigate their relationship in light of compliance with both instruments and whether that might lead to premature public disclosure. Their application, differences in timeframes and consequent potential conflict should be understood in the context of their different protection aims. Issues related to compliance under these two frameworks have sparked discussion since the adoption of NIS1 and GDPR. Entities falling under the scope of applicability of both instruments have voiced their opinions, contributing alongside other relevant stakeholders to the adoption of NIS2. The reporting obligations under NIS2 coexist without prejudice to those established by the GDPR.[10] Although the NIS2 and the GDPR provide for different requirements with different objectives, it is worth investigating their interplay since the same event might be notifiable under both frameworks.[11] The intersection in the applicability of reporting obligations might present significant challenges, particularly concerning early public disclosure of security breaches and its repercussions on incident response.[12]

The existing literature has addressed the relationship between the NIS1 and the GDPR, with the European Data Protection Supervisor (EDPS) also expressing that the former should

[9] Maria del Mar and Achiaga Negreiro, 'The NIS2 Directive - A high common level of cybersecurity in the EU' (2022) European Parliamentary Research Service, <https://www.europarl.europa.eu/thinktank/nl/document/EPRS_BRI(2021)689333> accessed 20 August 2023, 7-8

[10] 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 [2016] OJ L 119/1, Articles 32-34; Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Her, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 1, 9-10

[11] NIS Cooperation Group, 'Reference document on Incident Notification for Operators of Essential Services - Circumstances of Notification' (CG Publication, February 2018) <https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf> last accessed 27 October 2022 12-13; Sandra Schmitz-Berndt and Mark Cole 'The Interplay between the NIS Directive and the GDPR in a Cybersecurity threat landscape' (2019) University of Luxembourg Law Working Paper No. 2019-017

[12] Sandra Schmitz and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 101, 106-111

not prejudice the latter.[13] However, the EDPS does not clarify how to deal with potential conflicts between the two in cases where both notification obligations are triggered. Several academic articles have covered the topic of incident notification under NIS1 and many more investigated the data breach notification obligations (DBNO) under GDPR. In particular, the many relevant academic contributions of Sandra Schmitz-Berndt have been taken into consideration. Different journal articles present the general risk that these two instruments might generate incoherent obligations and lead to a lack of harmonization and thus diminished efficiency in the context of cybersecurity.[14] However, Schmitz-Berndt is the main reference for the argument that concurrent application of Article 23 NIS2 and 33-34 GDPR might lead to premature public disclosure of significant incidents. On the other hand, only one academic source was found that contravened these claims. This contribution, by Markopoulou, Papakonstantinou and de Hert (2019),[15] asserts that concerns over the double reporting frameworks are overstated and that if a conflict were to arise, it should be solved by reference to the different nature of NIS2 and GDPR as legal instruments and their different protection goals. However, to the best of my knowledge, there are no academic articles or secondary resources that address either side of the debate by using practical examples and case studies. The existing discussion remains on the surface level and relies on a theoretical analysis of the different parallel obligations, without taking a more practical approach. Furthermore, most existing resources examine the relationship between NIS1 and GDPR, while only a few take the NIS2 into account, due to its recent nature. In the future, further research will probably be more available, as well as new guidance and implementing acts.

The relevant legislative framework of the thesis is limited in scope to the European Union level, and it is constituted by the current NIS1, the NIS2, and the GDPR as its main primary sources. The secondary sources include journal articles, policy recommendations, opinions and assessment papers on the relevant subject. These come from both the public and the private sectors. The public sources include opinions of the European Data Protection

[13] European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (EDPS, 11 March 2021) https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf last accessed 1 October 2021 10-12

[14] Sandra Schmitz and Stefan Schiffner, 'Responsible Vulnerability Disclosure under the NIS 2.0 Proposal' (2021) 12 JIPITEC 447; Sandra Schmitz-Berndt and Mark Cole 'The Interplay between the NIS Directive and the GDPR in a Cybersecurity threat landscape' (2019) University of Luxembourg Law Working Paper No. 2019-017, Najmudin Saqib and others, 'Mapping of the Security Requirements of GDPR and NIS' (2020) School of Computer Science and Informatics, De Montfort University

[15] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review, 11

Supervisor, the European Data Protection Board, the Article 29 Working Party, and documents from national Data Protection Authorities (as defined below) and CSIRTs (Computer Security Incident Response Teams). Examples of private sources include documents created by individuals or groups of businesses and organizations to give opinions on the most practical aspects and issues of the implementation of the relevant regulatory framework.[16] It is noteworthy the positive credit rating that Moody's recently gave on the NIS2 and the overall developing cybersecurity requirements at the Union level.[17] The credit rating agency reported that the NIS2 will have stricter cybersecurity requirements met by companies within key economic sectors, thus improving their cyber resilience and incident response.[18] While this does not explicitly address the question of double reporting and the possible conflicts with Articles 33-34 GDPR, it still is an element that speaks in favour of NIS2. Most academic contributions used in this research will be of legal nature but some ICT and information security articles will also be considered. The merits of the literature can be judged against the aims of the selected sources and their relation to the present research question. They will contribute to the thesis in different ways: some sources will help build a general understanding of the background topic and the problem itself while others will allow a deeper insight by addressing the sub-questions and connecting the relevant findings.

However, the research presents some limits. The lack of existing extensive resources has been mentioned, particularly the absence of case studies and empirical evidence addressing the research topic steered the research into a more detailed and theoretical comparative analysis. As a consequence, the thesis is limited in the contribution to the production of an empirical-based investigation of the conflicting notification obligations and the issue of premature public disclosure. Nevertheless, this thesis aims at contributing to the literature in different ways. First off, a lot of research and attention has already been given to the GDPR

[16] Bitkom, 'Bitkom position on the proposal for a renewed Directive on security of network and information systems' (Bitkom, March 2021) <https://www.bitkom.org/sites/default/files/2021-03/210318_pp_nis-directive-2.pdf> accessed 8 August 2023; Niemann F, Karniyevich N and Sickinghe F, 'NIS2 Directive EU Co-legislators reach a provisional agreement' (Bird & Bird, June 2022) <https://www.twobirds.com/-/media/new-website-content/pdfs/insights/2022/global/220608_nis2-directive_provisional-agreement_newsletter_final.pdf> accessed 8 August 2023; European Banking Foundation, 'EBF key messages on the proposal for a Revised Directive on Security of Network and Information Systems (NIS2)' (EBF, June 2021) <https://www.ebf.eu/wp-content/uploads/2021/06/EBF-key-messages-on-NIS2-proposal.pdf> accessed 8 August 2023

[17] Moody's Investor Service, 'Cyber – Europe: New EU cybersecurity legislation is credit positive' (Moody's Investor Service, June 2022) https://admin.govexec.com/media/sector_comment_-_cyber-europe_-_14jun22.pdf accessed 8 August 2023

[18] Ibid

which has overshadowed the NIS 1 in the public and academic debate.[19] This is not just because of the immense popularity of the GDPR but also because the former is a Regulation and more principles-based, while the latter is a Directive containing more specific rules.[20] Therefore, it is interesting to research the relationship between these two instruments while putting the NIS1 as both the starting point and the centre stage of this project. Secondly, because as mentioned the NIS2 is a very recent development, there is not much research on it yet. Research on NIS2, therefore, is not redundant and allows this thesis to address the research question by building on the NIS1 experience and literature while reframing the problem of notification obligations and premature disclosure under the context of NIS2 and its important developments.

1.2. Research Question

In light of the above, the main research question of this thesis is: What is the relationship between the mandatory reporting obligations of significant incidents under NIS2 and data protection breaches under GDPR and how is this affected in light of premature public disclosure?

The sub-research questions that will be investigated are:

i. What is the overlap between the mandatory notifiable incidents under Articles 23 NIS2 and 33-34 GDPR?
ii. How do the notification obligations of Articles 23 NIS2 and 33-34 GDPR compare and relate in terms of applicability?
iii. To what degree do different timelines and parallel applicability give rise to premature public disclosure?

1.3. Thesis Overview and Methodology

This thesis is mostly based on secondary research and builds on a variety of primary and secondary sources. Its structure is designed to examine the notification obligations under NIS2 and GDPR through a consistent format across the four chapters. To answer the sub-questions, each chapter contains first a comprehensive descriptive part, based on primary sources, namely the legislative texts themselves. To allow a better insight into the provisions,

[19] Edward Machin, 'Events, dear boy: EU proposed new cyber law' (Ropes & Gray LLP, 16 May 2022) https://www.lexology.com/library/detail.aspx?g=b0552632-3506-4a25-a672-2e4e7829a1c7 accessed 10 August 2023

[20] Alessandro Mantelero, Giuseppe Vaciago, Maria Samantha Esposito and Nicole Monte, 'The common EU approach to personal data and cybersecurity regulation' (2020) 28 International Journal of Law and Information Technology, 297–328

references are made to the guiding documents provided by the relevant authorities under NIS2 and GDPR. On this foundation, the more analytical part is built, where a comparison is drawn between the different reporting requirements. This comparative analysis aims at exploring the key criteria, similarities, and differences between Articles 23 NIS2 and 33-34 GDPR, and ultimately outlining their relationship in Chapter 3. Comparative legal research as the main methodology will allow the descriptive and detailed analysis of the relevant legal rules on reporting obligations found in the selected primary sources, namely the NIS2 and the GDPR. The notification obligations of Article 23 NIS2 and Articles 33-34 GDPR were chosen as units of analysis. Their comparability was investigated based on their similar regulatory function as notification obligations (see Chapter 2.1), the possible overlap in notified incidents (Chapter 2.8), and their comparable structure/format (Chapter 3), albeit under different contexts and in the pursuit of different goals (Chapter 4.1). This thesis considers only mandatory reporting obligations, to the exclusion of voluntary reporting. The mandatory nature of the relevant rules allows for further comparability and emphasizes the potential challenge of their parallel application and compliance.

Chapter 2 will present notification obligations as a regulatory tool, and then investigate in particular the mandatory notifiable incidents under GDPR and NIS2. Gaining an overview of what triggers notification helps to see how this obligation can overlap for the same event under different aspects of information security and data protection. Chapter 3 will describe and compare in detail the procedural aspects of Article 23 NIS2 and Articles 33-34 GDPR. In particular, the different timelines are discussed, together with the importance of designing notification obligations that allow sufficient time for efficient compliance. The relationship between the two sets of obligations is investigated to clarify how they coexist and how applicability can arise in parallel.

Chapter 4 will address whether double reporting under notification obligations with different timeframes might adversely affect relevant entities' incident response in instances of early public disclosure. The argument of premature disclosure, as argued by Schmitz, will be presented. This will be done by analyzing the different interpretations of 'undue delay' under NIS2 and GDPR, which align with their distinct protection goals. Importantly, some key developments will be used to reframe the argument within the context of NIS2. A possible approach for dealing with the potential conflict between NIS2 and GDPR will be introduced, which draws on the contextualization of the nature of the legal instrument and the protection aims at stake.

The last and final chapter summarizes the overall findings and provides a conclusion to the main research question.

Chapter 2 - Mandatory Notifiable Incidents under NIS2 and GDPR

Within the adoption of a more harmonized and comprehensive framework for handling significant cybersecurity incidents under NIS2, notification obligations play a central role.[21] Chapter 2 initially presents them as a regulatory instrument, then describes the incidents triggering mandatory notification under NIS2 and GDPR. A clear view of their interpretation is critical to understand first individual notification, and then when reporting under both NIS2 and GDPR may be triggered by the same event.

2.1. Notification Obligations as a Regulatory Instrument

While the introduction of DBNO is relatively recent in the EU, notification obligations are now incorporated into multiple frameworks within the broader EU cybersecurity landscape.[22] Notification obligations are an integral part of incident response policies and, while they may differ among various instruments, they generally follow a similar template.[23] This usually includes the definitions of breaches/incidents, reporting entities, notified actors, and thresholds triggering notification.[24] It also includes exemptions and safe harbours, penalties, enforcement authorities and remedies.[25] The structure of notification obligations is made of complex technical features whose design choices significantly impact their effectiveness and nature, reflecting clear policy preferences and goals.[26]

The overarching goals of notification obligations are the protection of individuals affected by incidents, the incentivization of security compliance, and the increased awareness

[21] Maria del Mar and Achiaga Negreiro, 'The NIS2 Directive - A high common level of cybersecurity in the EU' (2022) European Parliamentary Research Service, <https://www.europarl.europa.eu/thinktank/nl/document/EPRS_BRI(2021)689333> accessed 20 August 2023, 7

[22] Sandra Schmitz-Berndt and Fabian Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context' (2021) 7 European Data Protection Law Review 101, 101-102

[23] Mark Verstraete and Tal Zarsky, 'Optimizing Breach Notification' (2020) 2021 University of Illinois Law Review 803, 809

[24] ibid

[25] Fabio Bisogni, Hadi Asghari and Michel van Eeten, 'Estimating the size of the iceberg from its tip: An investigation into unreported data breach notifications' (Proceedings of 16th Annual Workshop on the Economics of Information Security, La Jolla, 2017) https://pure.tudelft.nl/ws/portalfiles/portal/28437304/WEIS_2017_paper_54_2.pdf accessed 11 August 2023 4-5; Mark Verstraete and Tal Zarsky, 'Optimizing Breach Notification' (2020) 2021 University of Illinois Law Review 803, 809

[26] Mark Verstraete and Tal Zarsky, 'Optimizing Breach Notification' (2020) 2021 University of Illinois Law Review 803, 812

of existing security capacity and measures which allows for systematic feedback and the development of regulatory frameworks and enforcement strategy.[27]

However, there are challenges to their adoption, mainly trifold. First, the insufficient clarity of obligations and their boundaries.[28] Secondly, the lack of adequate incentives for compliance.[29] Thirdly, the unclear prioritization of efforts towards the highest threats.[30] In the context of this thesis, the first point holds the most relevance. The extensive scope of EU data protection and information security law necessitates specific and technical reporting regulations in order to provide legal certainty and maximize compliance of all activities and entities covered, particularly in light of the expansion brought about by NIS2.[31] Vague standards and interpretations can hinder effective prevention and response to incidents, as they leave excessive room for uncertainty in their application.[32] Timelines are particularly important and their design can substantially impact a notification obligation's outcome. If not adequately designed there is a risk that notifications will fail to provide sufficient technical details about the suffered incident, or that the information provided will not be correct or up-to-date.[33]

2.2. Significant Incidents under NIS2

[27] Fabio Bisogni, Hadi Asghari and Michel van Eeten, 'Estimating the size of the iceberg from its tip: An investigation into unreported data breach notifications' (Proceedings of 16th Annual Workshop on the Economics of Information Security, La Jolla, 2017) https://pure.tudelft.nl/ws/portalfiles/portal/28437304/WEIS_2017_paper_54_2.pdf 11 August 2023 3-4; Maria Karyda and Lilian Mitrou, 'Data Breach Notification: Issues and Challenges for Security Management' (10th Mediterranean Conference on Information Systems MCIS, Cyprus, 2016) https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1060&context=mcis2016 accessed 10 August 2023, 8

[28] František Kasl, 'The US lessons for the EU personal data breach notification' (2021) 11 The Lawyer Quarterly 195, 200-201

[29] Maja Nyman and Christine Große, 'Are You Ready When It Counts? IT Consulting Firm's Information Security Incident Management' (5th International Conference on Information Systems Security and Privacy ICISSP, Prague, 2019) https://www.sciencegate.app/document/10.5220/0007247500260037 accessed 10 August 2023, 30-35

[30] František Kasl, 'The US lessons for the EU personal data breach notification' (2021) 11 The Lawyer Quarterly 195, 200-201

[31] Ibid

[32] Ibid

[33] Information Technology Industry Council, Global Policy Principles for Security Incident Reporting (ITI, 27 September 2021) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf accessed 8 August 2023

Notification requirements are a central obligation to NIS2 and its goal of ensuring cybersecurity. The establishment of aligned reporting processes of relevant incidents to authorities is critical to ensure that NIS2 will account for the shortcomings of NIS1.[34]

There are multiple definitions of a cybersecurity incident, which can be classified based on their nature and impact.[35] NIS1 provided a widely used definition, based on an all-hazard approach and encompassing any event with an impact on the security of networks or information systems.[36] It included all types of impact, not distinguishing malicious from non-malicious incidents.[37] In this respect, NIS2 reduces fragmentation in two ways. First, by introducing a more specific notion of 'incident'.[38] Secondly, by giving a new interpretation to the threshold of significance that qualifies incidents as reportable, irrespective of whether the entity concerned is an important or essential entity.[39]

NIS2 requires all significant incidents to be notified.[40] Incidents are defined as any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.[41] An incident is significant if:

1) it caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;[42]
2) it has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material damage.[43]

Essential and important entities, to which NIS2 applies, must first establish an event as an incident and then assess its significance. Its significance is independent of the

---

[34] European Commission, 'Impact Assessment Report accompanying the document 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' (*European Commission, 16 December 2020)* 345 final, part 1/3 *https://ec.europa.eu/newsroom/dae/redirection/document/72176* accessed 20 August 2023, 32

[35] NIS Cooperation Group, 'Cybersecurity Incident Taxonomy' (CG Publication, July 2018) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646 accessed 8 August 2023, 6-8

[36] NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting' (CG Publication, April 2020) <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group> accessed 13 July 2023

[37] Ibid

[38] Sandra Schmitz-Berndt, 'Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes' in Cyricil Onwubiko et al (eds) *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (Springer 2023) 343, 345-346

[39] ibid

[40] Article 23(1) NIS2

[41] Article 6(6) NIS2

[42] Article 23(3)a NIS2

[43] Article 23(3)b NIS2

materialization of the damage: it is based on the potential of the incident to cause substantial harm or considerable loss.[44] This extension is an important departure from NIS1.[45] The European Parliament and different stakeholders have opposed to this, on the grounds that notification should be restricted to significant incidents that have caused actual harm.[46] Aside from mandatory notification under Article 23 NIS2, essential and important entities may voluntarily notify incidents, cyberthreats, and near misses, even when they do not qualify as significant.[47]

Entities falling outside the scope of NIS2 may also participate in the voluntary notification.[48] The voluntary system is a welcomed change from the NIS2 Proposal, which included significant cyber threats as mandatory notifiable incidents. This was problematic due to their broad definition under the EU Cybersecurity Act, which would have included even phishing and scam emails, thereby leading to excessive reporting, unwarranted given their risk level.[49] These incidents are now notifiable voluntarily and outside the research scope of this thesis, which focuses on mandatory reporting (under Article 23 NIS2). Both mandatory and voluntary reporting of obligations contribute to the overall information sharing, which NIS2 promotes.[50] This includes both information sharing from entities to authorities and among entities themselves. Gaining deeper insight into the overall threat landscape benefits authorities as well as entities.[51]

2.3. Personal Data Breaches under GDPR

[44] Sandra Schmitz-Berndt, 'Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes' in Cyricil Onwubiko et al (eds) *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (Springer 2023) 343, 346

[45] Sandra Schmitz-Berndt and Pier Giorgio Chiara, 'One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive' (2022) Int. Cybersecur. Law Rev. 289, 293

[46] European Banking Foundation, 'EBF key messages on the proposal for a Revised Directive on Security of Network and Information Systems (NIS2)' (EBF, June 2021) <https://www.ebf.eu/wp-content/uploads/2021/06/EBF-key-messages-on-NIS2-proposal.pdf> accessed 10 August 2023, 3

[47] Article 30(1)a NIS2

[48] Article 30(1)b NIS2

[49] Digital Europe, 'Harmonising cyber protection across Europe: The digital industry's basic asks for the NIS2 trilogues' (Digital Europe, February 2022) <https://www.digitaleurope.org/resources/harmonising-cyber-protection-across-europe-the-digital-industrys-basic-asks-for-the-nis2-trilogues/> accessed 10 August 2023, 5; European Banking Foundation, 'EBF key messages on the proposal for a Revised Directive on Security of Network and Information Systems (NIS2)' (EBF, June 2021) <https://www.ebf.eu/wp-content/uploads/2021/06/EBF-key-messages-on-NIS2-proposal.pdf> accessed 10 August 2023, 35

[50] Article 29 NIS2

[51] Florian Skopik, Giuseppe Settanni and Roman Fiedler, 'A problem shared is a problem halved: A survey on the dimension of collective cyber defense through security information sharing' (2016) 60 Computers & Security 154, 172-174

A personal data breach always originates with a security breach, which entails a vulnerability in the organisational or technical area of data security.[52] Data security encompasses three main aspects: confidentiality, integrity and availability.[53] Most data breaches will result in one or more aspects being threatened.[54] However, while all personal data breaches are security incidents, not all security incidents qualify as personal data breaches.[55] That is because not all of them involve personal data and GDPR only deals with data breaches affecting personal data.[56]A personal data breach is defined under Article 4(12) GDPR as a breach of security where both the definitions of personal information (any information relating to an identifiable natural person) and breach (destruction, loss, alteration, unauthorized disclosure of, or access to, data) are very broad.[57] Thus, GDPR deals specifically with security incidents which negatively affect personal data protection, which may in turn also have relevance for cybersecurity concerns.[58]

A breach can be either intentional as well as negligent.[59] Rather, what is relevant are its consequences, which are assessed using the above-mentioned three aspects of confidentiality, integrity and availability.[60] While confidentiality and integrity are easier to assess, availability breaches might not be as clear.[61] There is no standardized method for assessing all breaches.[62]

---

[52] Matthias De Bruyne, 'Data breach notification and the risk of over-notification. A comparative analysis of EU and US experiences in practice' (Master Thesis, Tilburg University 2016), http://arno.uvt.nl/show.cgi?fid=140479 accessed 8 August 2023, 11

[53] Ramakrishna Ayyagari, 'Data breaches and Carding' in Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrimeand Cyberdeviance* (Palgrave Macmillan 2020) 939, 940-941

[54] Matthias De Bruyne, 'Data breach notification and the risk of over-notification. A comparative analysis of EU and US experiences in practice' (Master Thesis, Tilburg University 2016), http://arno.uvt.nl/show.cgi?fid=140479 accessed 8 August 2023, 11

[55] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf accessed 11 August 2023, 8

[56] Ibid

[57] Article 4(12) GDPR

[58] Eva Schlehahn, 'Cubersecurity and the State' in Markus Christen, Ber Gordijn and Michele Loi (eds) *The Ethics of Cybersecurity* (Springer 2020) 205, 213

[59] Bernold Nieuwesteeg and Michael Faure, 'An analysis of the effectiveness of the EU data breach notification obligation' (2018) 34 Computer Law & Security Review 1232, 1234

[60] Ibid

[61] Mehmet Bedii Kaya, 'Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law' (2021) 70 Annales de la Faculté de Droit d'Instanbul 195, 205

[62] Ibid

Each assessment needs to be carried out case-by-case and according to the circumstances of each incident and the specific impact on personal data.[63]

The notification obligations, as provided by Articles 33-34 GDPR will be carried out depending on the actual impact of the data breach, as will be discussed in Chapter 3.2.

2.4. Important and Essential Entities

Under NIS1 national competent authorities (NCAs) identify which entities fall within its cope based on criticality criteria.[64] On the other hand, NIS2 adopts a simpler system based on entity size, whereby the burden of responsibility is shifted to the entities themselves, requiring them to self-identify for NIS2 applicability.[65] This new threshold is considered a good proxy to assess entities' importance and criticality within our economy and society.[66] As a result, NIS2 applies to medium-sized and larger public and private entities belonging to Annex I (essential entities, sectors of high criticality) and important entities as per Annex II (important entities, other critical sectors).[67] Generally, entities with less than 50 workers and an annual balance sheet of less than EUR 10 million will be excluded from applicability.[68]

However, despite the size-cap rule, certain entities listed in Annexes I and II may still fall under NIS2, regardless of their dimension. Member States may determine applicability of NIS2 for certain small and micro enterprises if they fulfil key roles for society, economy or particular sectors/services falling within the scope of NIS2.[69] The European Commission and the NIS Cooperation Group, established to support and facilitate cooperation and information exchange among Member States, are responsible to provide guidelines for the applicability criteria and guidance for these smaller enterprises.[70] Moreover, NIS2 also applies to entities classified as critical, independently of their size, and to entities providing domain name registration services.[71]

---

[63] Ibid, 205-206

[64] Thomas Sievers, 'Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations' (2021) 2 Int. Cybersecur. Law Rev 223, 225

[65] Valentino Lucini, 'The ever-increasing cybersecurity compliance in Europe: the NIS2 and what all businesses in the EU should be aware of' (2023) 11 Russian Law Journal 145, 146-147

[66] Thomas Sievers, 'Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations' (2021) 2 Int. Cybersecur. Law Rev 223, 226

[67] Article 2(1) NIS2

[68] Thomas Sievers, 'Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations' (2021) 2 Int. Cybersecur. Law Rev 223, 226

[69] Niels Vandezande, 'Cybsersecurity in the EU: how the NIS2-Directive stacks up against its predecessor' (KU Leuven - Centre for IT & IP Law, 2023) https://ssrn.com/abstract=4383118 last accessed 10 August 2023, 5-6

[70] Recital 7 and 20 NIS2

[71] Article 2(3) and 4 NIS2

Under NIS2, the NIS1 categories of "operators of essential services" (OES) and "digital service providers" (DSPs) are replaced by important and essential entities.[72] The new categorization is based on the sector to which an entity belongs, as specified in the Annexes, and entities are allocated to their corresponding category.[73] NIS2 covers essential entities from sectors of high criticality, such as energy, transport, finance, healthcare, water supply, digital infrastructure, public administration and space. It also covers other critical sectors (important entities): digital providers, postal services, waste management, foods, chemicals, manufacturing and research. Beyond the list of Annex I, entities may classify as essential based on further considerations. These include qualified trust service providers and top-level domain name registries, providers of public electronic communications networks or of publicly available electronic communications services, and public administration entities.[74] Entities referred to Annex I or II not qualifying as essential, including those as identified by Member States, will then be considered as important entities.[75]

Beyond the size-cap rule and the sector criterion, the applicability of NIS2 may depend on further considerations. For instance, public administration entities belong to Annex I and classify as essential entities, but they will be subjected to NIS2 only when entities of central government or of regional level, and when providing services, the disruption of which could have a significant impact on critical societal or economic activities.[76] Differently, public administration entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement will be excluded by NIS2.[77] Moreover, depending on the national implementation by Member States, NIS2 may apply also to local-level administrations, as well as educational institutions.[78]

Regarding notification obligations, there is no distinction in requirements for important and essential entities for significant incidents, which are the same. However, there are differences in the administrative fines for failure to report. Essential entities face fines to a maximum of €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[79] For important entities, fines amount to a maximum of at

[72] Articles 4(4) and 4(6) NIS1
[73] Sectors of high criticality under Annex I NIS2 and other critical sectors under Annex II NIS2
[74] Article 2(2) NIS2
[75] Article 3(2) NIS2
[76] Article 2(2)f NIS2
[77] Article 2(7) NIS2
[78] Article 2(5) NIS2
[79] Article 34 NIS2

least €7,000,000 or at least 1.4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[80]

2.5. Controllers, Joint Controllers and Processors

GDPR obligations are directed to controllers and processors. Controllers determine the purposes and means of personal data processing.[81] When this is done by two or more controllers jointly, they are considered joint controllers.[82] An example of joint controllership is found in the CNIL decision, where both Uber Technologies Inc. and Uber B.V. qualified as joint controllers due to their shared determination of data processing means and purposes.[83] Joint controllers are responsible for allocating their respective shared responsibilities under GDPR, including the notification obligations of Articles 33 and 34 GDPR.[84] This requires joint controllers to organize their actions and establish contractual arrangements determining how compliance is to be fulfilled, as suggested by WP29.[85]

While overall data protection responsibility rests primarily on controllers, processors also bear some responsibility and must facilitate compliance by controllers.[86] This includes obligations related to personal data breach notification.[87] Data processors are entities which process personal data on behalf of the controller.[88] Under Article 33 GDPR they are under the obligation of notifying a personal data breach to the controller without undue delay, after becoming aware. Once notified by the processor, the controller will then have to report the

---

[80] Ibid

[81] Article 4(7) GDPR

[82] Article 26 GDPR

[83] Elif Kiesow Cortez, 'Data Breaches and GDPR' in Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrimeand Cyberdeviance* (Palgrave Macmillan 2020) 239, 251

[84] Mehmet Bedii Kaya, 'Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law' (2021) 70 Annales de la Faculté de Droit d'Instanbul 195, 214; Najmudin Saqib and others, 'Mapping of the Security Requirements of GDPR and NIS' (2020) 7 School of Computer Science and Informatics, De Montfort University 20

[85] Mehmet Bedii Kaya, 'Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law' (2021) 70 Annales de la Faculté de Droit d'Instanbul 195, 214; European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 11 August 2023, 13

[86] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf accessed 11 August 2023, 13-14

[87] Ibid 13-14

[88] GDPR Art. 4(8)

breach to the competent supervisory authority or the data subject, if needed. While carrying out this obligation, the role of the processor is limited to the establishment of the breach and the notification to the controller.[89] It is then the latter who has to assess the likelihood of the risk presented by the breach.[90] Moreover, a processor may report a breach on behalf of the controller, if contractually authorized to do so.[91]

Therefore, processors also bear some responsibility for data infringement reporting.[92] Notwithstanding, the ultimate legal responsibility lies with the controller.

2.6. Competent national authorities and CSIRTs

Enforcement under NIS1 was proven ineffective.[93] Member States failed to apply penalties for failure to comply, also concerning incident notification obligations.[94] This prompted enforcement changes under NSI2, with a view to tightening supervision and defining more clearly the tasks and powers of the competent authorities.[95] Under NIS2, competent authorities, together with a single point of contact will be designated by Member States.[96] Notification obligations, under Article 23 NIS2, are primarily addressed to computer security incident response teams (CSIRTs) or, if applicable, the competent authority. Where the competent authority is notified, the Member State shall ensure that the notification will be forwarded to the CSIRT.[97]

Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-

[89] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf accessed 11 August 2023, 14

[90] Ibid 13

[91] Mehmet Bedii Kaya, 'Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law' (2021) 70 Annales de la Faculté de Droit d'Instanbul 195, 214-215

[92] Najmudin Saqib and others, 'Mapping of the Security Requirements of GDPR and NIS' (2020) 7 School of Computer Science and Informatics, De Montfort University 9-10

[93] Sandra Schmitz-Berndt and Pier Giorgio Chiara, 'One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive' (2022) Int. Cybersecur. Law Rev. 289, 294-295

[94] Ibid

[95] Maria del Mar and Achiaga Negreiro, 'The NIS2 Directive - A high common level of cybersecurity in the EU' (2022) European Parliamentary Research Service, <https://www.europarl.europa.eu/thinktank/nl/document/EPRS_BRI(2021)689333> accessed 8 August 2023, 6-7

[96] Article 8 NIS2

[97] Article 23(1) NIS2

border impact of the incident.[98] Member States may adopt a decentralized approach and establish different competent authorities for the relevant different sectors.[99] However, this may lead to fragmentation and make the identification of the relevant competent authority less straightforward. CSIRTs are responsible for incident handling, and together with competent authorities are given under NIS2 a very active role and deep involvement in the incident-handling process.[100]

2.7. Data Protection Authorities

Enforcement of the obligations set by GDPR mainly lies within the jurisdiction of EU member states' data protection authorities (DPAs).[101] DPAs are independent public bodies responsible for enforcing the GDPR and for imposing fines and sanctions for non-compliance.[102] Member States establish their own DPAs.[103] Each national DPA is competent for the tasks and powers assigned under GDPR on the territory of its own Member State.[104] Notification obligations under Article 33 GDPR are addressed to the DPAs: controllers must notify the competent data protection authority. Moreover, DPAs can request controllers to report a data breach to the data subject based on their own judgment.[105]

In practice, breaches often involve the processing of personal data in several Member States, giving rise to competence to multiple DPAs.[106] In cases of cross-border breaches, only one national DPA is the lead authority and is responsible on behalf of all other DPAs.[107] Based on the one-stop-shop competence mechanism, one lead DPA will act as the sole contact point

---

[98] Ibid

[99] Irene Kamara and Jasper van den Boom, 'Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices' (2022) TILT Tilburg Law School, 7-8

[100] Articles 10-11 NIS2

[101] Brian Daigle & Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' (2020) Journal of International Commerce and Economics 5-6

[102] Article 51 GDPR

[103] Brian Daigle & Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' (2020) 1 Journal of International Commerce and Economics 5-6; Detlev Gabel and Tim Hickman, 'Chapter 14: Data Protection Authorities – Unlocking the EU General Data Protection Regulation' (White & Case, 5 April 2019) https://www.whitecase.com/insight-our-thinking/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection accessed 17 August 2023

[104] Article 55(1) GDPR

[105] Article 58(2)e GDPR

[106] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (1st edn, Springer 2017) 190

[107] Ibid 192

for the controller/ processor whose processing activities affect multiple EU Member States.[108] The lead supervisory authority is the DPAs of the main (or single) establishment of the controller/processor.[109]

2.8. The Overlap Between Notifiable Incidents and Notifying Entities

Significant incidents often include personal data breaches: it was estimated that over 45% of security breaches involve personal data.[110] It is projected that the extended scope of NIS2 will lead to a notable increase in personal data processes for cybersecurity purposes.[111] This raises the question of whether the same event might have to be notified under both NIS2 and GDPR. However, while all personal data breaches are information security incidents, not all information security incidents are personal data breaches.[112] For instance, a denial of service attack on a NIS2 relevant entity's public-facing informational website would be an information security incident and could constitute a significant incident under NIS2 if the significance threshold is met.[113] However, it may not amount to a personal data breach as probably no personal data would have been posted on the website.[114]

As relevant entities under NIS2 might at the same time act as controllers and processors under the GDPR, they will have to comply with both frameworks with respect to their different (albeit concurrent) roles. However, the overlap between significant incidents and personal data breaches is not always self-evident.[115] Entities may fail to recognize the relevance under GDPR of the data processed by their cybersecurity systems and services.[116] This may include, without

---

[108] Ibid 191

[109] Article 56(1) GDPR

[110] Verizon, '2021 Data Breach Investigation Report' (*Verizon.com*, 2021) https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx accessed 8 August 2023

[111] European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (EDPS, 11 March 2021) https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf accessed 11 August 2023, 11

[112] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf accessed 8 August 2023, 7-8

[113] Annika Andreasson and Nicole Fallen, 'External Cybersecurity Incident Reporting for Resilience' in Jelena Zdravkovic et al (eds), *Perspectives in Business Informatics Research* (Springer Cham 2018) 4, 8

[114] Ibid

[115] European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (EDPS, 11 March 2021) https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf accessed 11 August 2023, 11

[116] Ibid

limitation, IP addresses, device identifiers, network log files, or access control log files[117] Comparing the notification criteria, it is noteworthy that notification under both GDPR and NIS2 does not require materialization of harm. Under GDPR the notification criteria refer to the connection of the data breach to the establishment of risk for the rights and freedoms of natural persons under Article 33, and to the threshold of high-risk under Article 34 GDPR.[118] Under NIS2 Article 23 potential (significant) harm sets the threshold. Therefore, significant incidents and personal data breaches trigger reporting based on a risk assessment that does not require actual harm to occur.

2.9. Conclusion

Chapter 2 answers the question of what are the notifiable incidents under NIS2 and GDPR, with a view to finding their intersection. This is the first step to understanding the applicability of notification obligations under NIS2 and GDPR. This was done by describing the notions of significant incidents and personal data breaches and discussing how they can overlap, based on their working provision, as well as guidance issued by the EDPS. Given that most security incidents involve personal data, it is worth exploring what the NIS2 and GDPR's reporting obligations exactly entail in terms of content, format and timeframes. Their similarities, differences and the nature of this parallel notification framework will be discussed in Chapter 3.

[117] Ibid

[118] Mario Renna, 'Data Breach Disclosure Duties' (2019) 2 European Journal of Privacy Law & Technologies 2 (2019) 79, 83

Table 1: Overview of mandatory notifiable incidents, notified authorities and notifying entities under GDPR and NIS2

Legislation	**GDPR**	**NIS2**
Terminology	Personal data breach	Incident
Definition	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 (Art. 4 (12) GDPR)	Any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems (Art. 6(6) NIS2)
Notification Criteria	All personal breaches must be notified to the SA - Unless they are not likely to result in a risk to the rights and freedoms of natural persons (Art. 33 GDPR) Personal breaches must be communicated to the data subject - If they are likely to result in a high risk to the rights and freedoms of natural persons (Art. 34 GDPR)	Significance: (Art. 23(3) NIS2) - It has caused/has the potential to cause severe service disruption or loss for the entity concerned - It has affected/has the potential to affect other persons by causing considerable damage
Notified authorities	Supervisory authority (SA), an independent public authority which is established by a Member State (Art. 4(21) GDPR)	CSIRTs/national competent authority, based on which is competent to receive the notification (Arts. 8(1) and 10(1) NIS2)
Notifying entities	Controllers, joint controllers and processors (Art. 4(7-8) GDPR)	Essential and important entities (Art. 3(1-2) NIS2)

Chapter 3 – Comparing Notification Obligations

Chapter 2 presented the triggering incidents for mandatory notification under NIS2 and GDPR, with the relevant notifying actors and authorities. Chapter 3 will describe and compare the procedural aspects of the notification systems of Article 23 NIS2 and Articles 33-34 GDPR. It aims to investigate the key criteria and highlight the similarities and differences to delineate their relationship.

3.1. Incident Reporting under Article 23 NIS2

The incident reporting obligations introduced by NIS1 are now streamlined by the three-tiered framework of Article 23 NIS2. Article 23 NIS2 establishes that significant incidents must be reported to the CSIRT or, where applicable, the competent authority following these three steps:

I. First, concerned entities must file an initial early warning without undue delay, and in any event within 24 hours of becoming aware of the significant incident. Where applicable, this early warning should indicate if the incident is suspected to have an unlawful or malicious cause and its potential cross-border impact.[119]

II. Secondly, entities must submit an incident notification without undue delay, and in any event within 72 hours of becoming aware of the significant incident. The purpose is updating the information from the early warning and conducting an initial assessment. This includes, where applicable, information on its severity, impact and indicators of compromise.[120]

III. Finally, a comprehensive report must be submitted within one month after the notification report (Step II). It must at least include a detailed description of the incident, its severity and impact. It should also address the likely type of threat or root cause, the mitigation measures (taken and ongoing), and where applicable, the cross-border impact.[121]

If by submission of the comprehensive report, the incident is still ongoing, another comprehensive report must be produced at this time, as well as a final report within one month

[119] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80, Art. 23(4)a
[120] Art. 23(4)b NIS2
[121] Art. 23(4)d NIS2

after the incident has been handled.[122] Moreover, upon request of a CSIRT or the competent authority, an intermediate report on the relevant status update can be requested.[123] Notifications are primarily addressed to the CSIRTs and the competent authorities. However, where significant incidents are likely to adversely affect the provision of their service, entities must also notify their service recipients without undue delay.[124] In the scenarios of cross-border or cross-sectoral significant incidents, the single points of contact of Member States must receive in due time the relevant information forwarded under the notification process.[125]

3.2. Incident Reporting Obligations under Articles 33-34 GDPR

The reporting obligations are found in Chapter 4 GDPR, which establishes the obligations of controllers and processors. Art. 33 GDPR establishes that personal data breaches must be notified by data controllers to the supervisory authority without undue delay and, where possible, within 72 hours from the moment they become aware of the breach. When the 72-hour threshold cannot be respected, the reasons for the delay should be stated and additional information may be added later on.[126] Article 34 GDPR requires notification of the data subject without undue delay when the breach is likely to result in a high risk to the rights and freedom of individuals. The circumstances of the breach should be taken into account, including the appropriate technical protection measures that the controller may have taken to prevent the breach and limit the potential damage.[127] To ascertain that the breach notification was forwarded without undue delay the nature and gravity of the breach should be considered, as well as its consequences and adverse effects on the data subject.[128] The assessment of high-risk under Article 34 GDPR should be objective.[129] Different factors should be included, as recommended by the EDPB, like the type of breach, the nature, sensitivity, and volume of data, the ease of identification of individuals, the severity of consequences for individuals, the special characteristics of the individuals and of the data controller, and the number of affected individuals.[130] The assessment should focus only on the specific risk and circumstances of each

[122] Art. 23(4)e NIS2
[123] Art. 23(4)c NIS2
[124] Art. 23(1) NIS2
[125] Art. 23(1) NIS2
[126] Recital 85 GDPR; Article 29 Data Protection
[127] See Recital 88 GDPR on the Format and Procedures of the Notification. Meaning whether the controller was already responsible and compliant
[128] Recital 87 GDPR on the promptness of reporting/notification.
[129] Recital 76 GDPR
[130] Recitals 75 and 76 of the GDPR, European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-

breach, taking into account how severe and likely it is for such risk to materialize.[131] The threshold is higher than for the notification to the supervisory authority.[132] It has a different focus than a DPIA as it focuses on the actual breach, already occurred event and the resulting risk of the impact of the breach.[133] The EDPB Guidelines provide detailed guidance on how to assess high-risk under Art. 34, and Annex B provides a list of examples.[134] When in doubt, controllers should tend to pay extra caution and pursue notification.[135] The Supervisory Authority should closely cooperate and guide the controller with the communication.[136]

Under certain circumstances, controllers might be exempted from specific aspects of the notification obligations. Notification under Article 33 GDPR is not required when the breach is unlikely to present a risk to the rights and freedoms of natural persons. For instance, where personal data have already been made publicly available, their disclosure would not pose a likely risk and therefore would not warrant a notification.[137] This is the case where data is manifestly and deliberately made public by the data subject, by publicly posting it on social media or on a public internet page. Therefore, in this scenario the level of availability or publicity of the data is not altered by the breach.[138] It should be noted that while notification might not be initially necessary, the risk could have to be re-evaluated later and based on that the notification could be triggered at a later stage.[139] On the other hand, notification to the data

---

10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 13

[131] Ibid

[132] Bernold Nieuwesteeg and Michael Faure, 'An analysis of the effectiveness of the EU data breach notification obligation' (2018) 34 Computer Law & Security Review 1232, 1234

[133] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (Article 29 WP, 6 February 2018) https://ec.europa.eu/newsroom/article29/redirection/document/49827 accessed 8 August 2023, 23

[134] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (Article 29 WP, 6 February 2018) https://ec.europa.eu/newsroom/article29/redirection/document/49827 accessed 8 August 2023, 31-33

[135] Ibid, 26

[136] Recital 86 GDPR

[137] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 19

[138] Article 29 Data Protection Working Party, 'Opinion 03/2014 on Personal Data Breach Notification' (Article 29 WP, 25 March 2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf accessed 8 August 2023, 14-15

[139] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf accessed 8 August 2023, 19

subject under Article 34 GDPR is not necessary under three scenarios.[140] First, when the appropriate technical and organisational protection measures have been implemented by the controller and applied to the personal data affected by the breach so that the concerned personal data was made unintelligible to any person who is not authorised to access it.[141] For instance, by means of encryption of personal data.[142] Second, when it is ensured that harm to the rights of data subjects will no longer materialise based on the actions taken by the controller after the breach.[143] Third, when notification would require disproportionate effort on behalf of the controller. In this case, data subjects can be informed through other means.[144]

Regarding the content of the notification under Art. 33 GDPR, the information forwarded must at least include the nature of the personal data breach, the categories and the approximate number of data subjects and personal data concerned, the likely consequences of the breach, and the measures that the controller has taken or intend to take to address the breach and mitigate its potentially harmful consequences.[145] The name and contact details of the DPO or other relevant contact points should also be provided. This list of minimum required information ensures that the supervisory authority might take necessary action. The notification to the data subjects under Article 34 GDPR must include the description of the breach and similar information as under Article 33 GDPR, which shall be provided in clear and plain language.[146] A cooperation mechanism under Article 60 GDPR will come into play for cross-border data breaches: the lead authority will cooperate with the other supervisory authorities and exchange relevant information.[147] Finally, it must be noted that while the obligations address primarily controllers, processors also bear some responsibility for notification obligations, as discussed in Chapter 2.

3.3. A Relationship of Coexistence

Chapter 3 will now investigate the similarities between the NIS2 and the GDPR's reporting obligations. Their relationship has been contested as a source of legal uncertainty

[140] Article 34(3) GDPR
[141] Ibid
[142] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (1st edn, Springer 2017) 70
[143] Article 34(3) GDPR
[144] Ibid
[145] Article 33(3) GPDR
[146] Article 34(2) GDPR
[147] Article 60 GDPR

over compliance, potential regulatory issues and cumbersome administrative burden.[148] Already under NIS1 the question was raised on how entities would comply with both NIS1 and GDPR without discrimination and deal with potentially conflicting obligations.[149] The NIS2 applies without prejudice to the GDPR, as clarified in Article 2(12) and as welcomed by the observation of the EDPS.[150] Indeed, data protection as regulated by the GDPR applies to any processing of personal data falling within the scope of NIS2 and is not limited to specific contexts.[151] This is also reflected by the corresponding Recital 14, as suggested by the EDPS.[152] The reporting obligations of the two instruments, whilst appearing similar, are not mere duplications. Article 23 NIS2 does not exclude Articles 33-34 GDPR, nor vice versa.[153] The GDPR is not a lex specialis to the NIS2, which would then exclude the application of the NIS2. The GDPR introduces a notification obligation when personal data is involved, rather than regulating the security or notification requirement of significant incidents in the context of NIS2.[154] Thus, all data controllers must comply with the GDPR and report personal data breaches, while at the same time all relevant entities must report significant incidents under the NIS2: a breach of personal data is an issue in and of its own. Therefore, the same incident may be reported under two different frameworks, to two different regulators with two different aims: protection of personal data under the GDPR and protection of the underlying infrastructure under the NIS2. The EDPB Guidelines 9/2022 provide guidance on the GDPR notification of

[148] Niels Vandezande, 'Cybsersecurity in the EU: how the NIS2-Directive stacks up against its predecessor' (KU Leuven - Centre for IT & IP Law, 2023) https://ssrn.com/abstract=4383118 last accessed 10 August 2023, 4 and 15, Polona Car and Stefano de Luca, 'EU Cyber resilience act' (EPRS, 2022) https://www.dimt.it/wp-content/uploads/2022/12/EPRS_BRI2022739259_EN.pdf accessed 8 Augusto 2023, 11

[149] Najmudin Saqib and others, 'Mapping of the Security Requirements of GDPR and NIS' (2020) 7 School of Computer Science and Informatics, De Montfort University 1. Note that his concerns is not unique to the NIS2 and the GDPR. Similar discussions exists over other pieces of EU legislation which present comparable notification obligations coming into play with each other. See: NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting CG Publication 04/20' (NIS Cooperation Group, December 2020) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72147 last accessed 8 August 2023

[150] European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (EDPS, 11 March 2021) https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf last accessed 1 March 2022 October 2022, 10

[151] European Data Protection Supervisor, 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' (EDPS, 11 March 2021) https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf last accessed 1 March 2022 October 2022, 17

[152] Ibid

[153] Sandra Schmitz-Berndt and Fabian Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context'(2021) 7 Eur. Data Prot. L. Rev. 101

[154] Sandra Schmitz and Stefan Schiffner, Responsible Vulnerability Disclosure under the NIS 2.0 Proposal, 12 (2021) JIPITEC 447, 451-452.

obligations and how they relate to notifications schemes under other legal instruments.[155] Controllers must be aware of other parallel requirements to notify security incidents which are separate from the GDPR. On the other hand, competent NIS2 authorities and the supervisory authority under GDPR are required to cooperate and exchange information.[156] However, where security incidents involve personal data breaches, the relevant operators and/or providers have to notify the breach under the GDPR in a separate procedure from the incident notification under the NIS1 and under the NIS2 when it will enter into force.[157] To showcase this the EDPB Guidelines 9/2022 use the example of a cloud service provider which notifies of a breach under the NIS1 but may also need to notify a controller in case a personal data breach is involved.[158]

The question is then raised of whether compliance to both NIS2 and GDPR might cause conflicts and confusion when the same incident is reported by the relevant service provider and controller (which could be the same entity, acting in different capacity), to two different authorities under two reporting frameworks providing for a different format, content and timelines.[159] These similar yet different reports might lead to authorities receiving contrasting information.[160] The same incident could then be treated as two separate ones if there is insufficient communication and cooperation between the two authorities.[161] However, the focus of this thesis is on the relationship between the two reporting obligations as based on the divergence in their timelines and the resulting implications. More specifically, whether that may lead to the premature notification of users and public disclosure of incidents, which in turn might have negative effects on cybersecurity and the overall protection goal of NIS2.[162] It should be recognized that the NIS2 framework is different compared to NIS1. Indeed, one core goal of NIS2 was to streamline the EU approach and facilitate overall compliance while

[155] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 27-28

[156] Art. 31(3) and Recital 136 NIS2

[157] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 28

[158] Ibid

[159] Sandra Schmitz-Berndt and Mark Cole 'The Interplay between the NIS Directive and the GDPR in a Cybersecurity threat landscape' (2019) University of Luxembourg Law Working Paper No. 2019-017

[160] Ibid

[161] Sandra Schmitz-Berndt and Fabian Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context'(2021) 7 Eur. Data Prot. L. Rev. 101

[162] Sandra Schmitz and Stefan Schiffner, Responsible Vulnerability Disclosure under the NIS 2.0 Proposal, 12 (2021) JIPITEC 447, 451-452

reducing fragmentation.[163] Therefore, the concerns and arguments on the NIS1-GDPR relationship, one of which is premature user notification, should now be revised and contextualized under the updated NIS2 legislative framework. Almost all existing literature on this refers to the NIS1 or the NIS2 Proposal for the most recent sources. This thesis draws from these sources and arguments while taking into account the new NIS2 provisions, reframing the discussion and addressing eventual developments.

3.4. The Main Differences between Reporting Obligations

One first departure between the two notification obligations is their intended recipients: NIS2 establishes notification to the CSIRTs or where applicable, the competent authority and where appropriate, to the recipients of their services.[164] On the other hand, notification of a personal data breach under the GDPR is addressed to the supervisory authority competent, and potentially to data subjects if the breach poses a high risk.[165] This difference in notification recipients is tied to the rationale and protection aims of NIS2 and GDPR.[166] NIS2 aims at the re-establishment of information security systems and cybersecurity is the forefront goal. Therefore, individuals affected by a significant incident will be notified only when the public is informed about the accident by the concerned Member State's CSIRT or, where applicable, its competent authority.[167] This would be the case when public awareness is necessary to prevent or deal with an ongoing significant incident, or when disclosure is in the public interest.[168] Under NIS2, the direct focus is not on the individual natural persons involved. Conversely, the GDPR's notification goal is to inform the data subjects, and provide them with assistance and protection from the possible risks and consequences stemming from the data breach.[169] The protection of the rights and freedoms of natural persons is the forefront, together

[163] Sandra Schmitz-Berndt and Mark Cole 'The Interplay between the NIS Directive and the GDPR in a Cybersecurity threat landscape' (2019) University of Luxembourg Law Working Paper No. 2019-017; Sandra Schmitz-Berndt and Fabian Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context'(2021) 7 Eur. Data Prot. L. Rev. 101.

[164] Article 23(1) NIS2

[165] Articles 33 and 34 GDPR

[166] Annika Andreasson and Nicole Fallen, 'External Cybersecurity Incident Reporting for Resilience' in Jelena Zdravkovic et al (eds), *Perspectives in Business Informatics Research* (Springer Cham 2018) 4, 13-14

[167] Sandra Schmitz and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 101, 102-103

[168] Article 23(7) NIS2

[169] Recital 75 and 85 GDPR on possible risks

with the empowerment of individuals to protect themselves and mitigate risk.[170] The difference in protection goals may potentially lead to one undermining the other when compliance with both is required for the same event.[171] However, they are not just contradictory nor repetitive, and instead, they should be understood in relation to both data protection and information security.[172] Chapter 4 will address the issue of premature public disclosure, where GDPR's emphasis on prompt notification of data subjects, as aligned with the overarching aim of protecting individuals' rights and freedom, plays a central role.[173] A second divergence relates to the content of the notification. NIS2, when compared to NIS1, defines more clearly the information to include when reporting a significant incident.[174] Especially in regard to the third and final report, for which a list of the minimum information is provided.[175] However, the content under Article 23 NIS2 is still less precisely defined than under GDPR, which requires more specific and detailed information. This can be explained by the layered framework of NIS2, which progressively requires more information based on the development of the incident and its investigation. This facilitates the gradual collection and update of data. Additionally, CSIRTs can offer guidance as to what information is relevant in a specific reporting procedure, other than requesting an interim report.[176] Moreover, notifications under GDPR and NIS1 require different information to be notified content-wise, as they have different underlying purposes. The third and most contentious departure between Article 23 NIS2 and Articles 33-34 GDPR revolves around their different timelines. Both instruments use the notion of undue delay in the context of reporting obligations' timeframes. Under NIS1, 'undue delay' was the only time reference given for reporting obligations, while now under NIS2 this standard is combined with the 24 hours deadlines for the early warning, and the 72 hours for the incident notification report.[177] This reduces the fragmentation caused by NIS1's broad discretion, which

[170] Sandra Schmitz-Berndt and Fabian Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context'(2021) 7 Eur. Data Prot. L. Rev. 101

[171] Sandra Schmitz and Stefan Schiffner, Responsible Vulnerability Disclosure under the NIS 2.0 Proposal, 12 (2021) JIPITEC 447, 457

[172] Ibid

[173] Recital 87 GDPR; Article 34 GDPR; European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 20

[174] Articles 14 and 16 NIS1; Article 23(4) NIS2

[175] Article 23(3)d NIS2

[176] Articles 11(3) and 23(3)c NIS2

[177] Sandra Schmitz-Berndt and Pier Giorgio Chiara, 'One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive' (2022) Int. Cybersecur. Law Rev. 289, 293

resulted in widely different interpretations and requirements among Member States.[178] Under GDPR the concept of 'undue delay' remains quite abstract, and is vaguely defined by Recital 86 as 'as soon as reasonably feasible'.[179] However, it is complemented with a 72 hours timeframe for notification to the DPA, to be complied with when feasible.[180] When designing the timeline for incident reporting, policymakers should consider global best practices and the diverse levels of incident severity. Based on that, an agreement by different stakeholders has been reached that a minimum of 72-hour should be given to entities for reporting.[181] A shorter window would be too constraining, and potentially compromise the quality and accuracy of the information reported, while also increasing the overall complexity of incident investigating and reporting.[182] This could hamper cybersecurity standards and limit the efficacy of incident response efforts.[183] The 24 hours timeline provided under the NIS2 Proposal was criticized and deemed insufficient for any incident type, and unfeasible for businesses to comply with.[184] In the first critical 24 hours after an attack, entities should devote their resources to mitigating the incident instead of diverting them to produce a report for the sake of legal compliance.[185] Rather, they should strive for the identification and response to the incident, remedying the attack and protecting of their business continuity.[186] However, incident reporting and even more so information sharing can be beneficial for cases of multi-party attacks, where

[178] Sandra Schmitz and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology, 4

[179] Recital 86 GDPR

[180] Article 33(1) GDPR

[181] Bitkom, 'NIS Directive 2.0 – Bitkom Position' Bitkom position on the proposal for a renewed Directive on security of network and information systems' (Bitkom, 3 January 2022) https://www.bitkom.org/sites/default/files/2022-01/03.01.22_bitkom_nis2_positionspapiertrilog.pdf accessed 8 August 2023, 10; Information Technology Industry Council, *Global Policy Principles for Security Incident Reporting* (ITI, 27 September 2021) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf accessed 8 August 2023, 7

[182] Information Technology Industry Council, *Global Policy Principles for Security Incident Reporting* (ITI, 27 September 2021) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf accessed 8 August 2023, 5-6

[183] Ibid

[184] Information Technology Industry Council, 'ITI Recommendations for the NIS2 Trilogue Negotiations' (ITI, 8 February 2022) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf 11 August 2023, 5

[185] Digital Europe, 'Harmonising cyber protection across Europe: The digital industry's basic asks for the NIS2 trilogues' (Digital Europe, February 2022) <https://www.digitaleurope.org/resources/harmonising-cyber-protection-across-europe-the-digital-industrys-basic-asks-for-the-nis2-trilogues/> accessed 10 August 2023, 5-6

[186] Information Technology Industry Council, 'ITI Recommendations for the NIS2 Trilogue Negotiations' (ITI, 8 February 2022) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf 11 August 2023, 5

cybersecurity incidents involve different organizations and create cascading effects.[187] These ripple events entail a significant damage escalation, as the security breach is propagated.[188] In these scenarios, information sharing is key to incident response. Otherwise, entities would lose valuable time and effort by responding to the attack without sharing relevant information.[189] Information silos prevent sharing experiences, conducting cross-sector analysis and aggregating insights.[190] This may hinder incident response, whether between individual companies, across sectors, or internationally. It is then paramount to establish trustworthy platforms and infrastructure where organizations can share information. Under NIS2, this is promoted by the role of CSIRTs as information-sharing partners and by information-sharing arrangements under Article 29 NIS2. [191] Several information-sharing initiatives exist, which can be between private or public actors, sectoral or cross-sectoral.[192] Nevertheless, given the sensitive nature of information is important to ensure that entities will share information related to a multi-party attack within a trusted environment and that information-sharing will not backfire.[193] Secondly, this might be counter-productive, as entities and their customers would be exposed to an even bigger risk of further attacks if information about the incident is shared before the attack, mitigated and handled. This concern is closely linked to the potential issue of premature disclosure of incidents. Thirdly, rushing a notification report might lead to entities producing a higher volume of inaccurate or erroneously contextualized information, compared

[187] Jeff Burt, 'Multi-Party Cyberattacks Lead to Big Losses: Security Researchers' (eSecurity Planet, 21 October 2021) https://www.esecurityplanet.com/threats/multi-party-cyberattacks-lead-to-big-losses/ accessed 20 August 2023

[188] Cyentia, 'Information Risk Insights Study (IRIS) Tsunami – Following the wake of damage from major multi-party cyber incidents' (Cyentia, 2021) https://www.cyentia.com/wp-content/uploads/IRIS-Tsunami.pdf accessed 20 August 2023, 4-7

[189] Cyentia, 'Information Risk Insights Study (IRIS) Tsunami – Following the wake of damage from major multi-party cyber incidents' (Cyentia, 2021) https://www.cyentia.com/wp-content/uploads/IRIS-Tsunami.pdf accessed 20 August 2023, 17

[190] NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting' (CG Publication, April 2020) <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group> accessed 8 August 2023, 19

[191] Article 11(3)b NIS2

[192] National Cyber Security Centre, 'Exploration of best practices for cybersecurity information sharing' (*NCSC-NL)* https://english.ncsc.nl/research/research-results/exploration-of-best-practices-for-cybersecurity-information-sharing-map last accessed 8 August 2023

[193] Dimitrios D Skias et al, 'Demonstration of alignment of the Pan-European Cybersecurity Incidents Information Sharing Platform to Cybersecurity policy, regulatory and legislative advancements' (17th International Conference on Availability, Reliability and Security ARES, New York, 2022) https://dl.acm.org/doi/pdf/10.1145/3538969.3544477, 3-5; Important factors are the expertise, trust, membership requirements and structural design of the information-sharing environment: National Cyber Security Centre, 'Exploration of best practices for cybersecurity information sharing' (*NCSC-NL)* https://english.ncsc.nl/research/research-results/exploration-of-best-practices-for-cybersecurity-information-sharing-map last accessed 8 August 2023

to a scenario in which they would be allowed a longer time to perform. This would be especially challenging for SMEs enterprises.[194]

For all these reasons the changes made from the Proposal to the final NIS2 text appear beneficial.[195] The 24-hour timeframe only refers to an early warning, not to a proper report, which instead is requested within 72 hours. Entities will still be able to submit their reports earlier than the 72 hours deadline if able to, and authorities will receive overall more precise and error-free information, while also being able to better deal with the number of reports received.[196] A flexible approach has been advocated for the reporting obligations under NIS2, particularly concerning the time allowed for the final report.[197] Indeed, it is important for the timelines to be feasible so that entities can provide complete, correct and updated information. Before the first 72 hours, the available information might be too limited.[198] Thus, additional time and effort are required for entities to perform thorough investigations of significant incidents. As also recommended by the European Parliament, the timeline for the final comprehensive report should not be shorter than one month from the initial notification.[199] Moreover, since in some cases an incident or its investigation may still be ongoing when the comprehensive report is forwarded, it should be possible for entities to then submit one extra final report after the incident is completely settled.[200]

3.5 Conclusion

In Chapter 3, the reporting obligations of Articles 23 NIS2 and 33-34 GDPR were described and compared in terms of recipients, content and timeframes. In particular, the design of timelines was addressed as crucial for the effectiveness of the notifications. Indeed, entities necessitate sufficient time to gather and investigate the available information after an incident

[194] Digital Europe, 'Harmonising cyber protection across Europe: The digital industry's basic asks for the NIS2 trilogues' (Digital Europe, February 2022) <https://www.digitaleurope.org/resources/harmonising-cyber-protection-across-europe-the-digital-industrys-basic-asks-for-the-nis2-trilogues/> accessed 10 August 2023, 5

[195] Bitkom, 'NIS Directive 2.0 – Bitkom Position' Bitkom position on the proposal for a renewed Directive on security of network and information systems' (Bitkom, 3 January 2022) https://www.bitkom.org/sites/default/files/2022-01/03.01.22_bitkom_nis2_positionspapiertrilog.pdf accessed 8 August 2023, 10

[196] Information Technology Industry Council, 'ITI Recommendations for the NIS2 Trilogue Negotiations' (ITI, 8 February 2022) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf 11 August 2023, 5

[197] Ibid 6

[198] Ibid 5

[199] Information Technology Industry Council, 'ITI Recommendations for the NIS2 Trilogue Negotiations' (ITI, 8 February 2022) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf 11 August 2023, 6

[200] Ibid

is established in order to comply with the reporting obligations. However, excessive time and effort should not be diverted from the overarching goal of NIS2, namely the restoration of information security systems and of cybersecurity. The Chapter emphasized the key similarities and differences, analyzing their relationship and their coexistence as reporting frameworks. Indeed the application of one does not exclude the other and the same event might have to be notified under both the different reporting procedure and timelines of NIS2 and GDPR.

Chapter 4 – Premature Public Disclosure Based on the Context of NIS2

Chapter 3 described the importance for relevant entities and controllers to be given sufficient time to comply with reporting obligations.[201] Chapter 4 discusses whether the different time requirements between NIS2 and GDPR may cause premature public disclosure of incidents. The important developments brought by NIS2 and their effects in this context are duly considered.

4.1. The Different Protection Aims Behind the Different Timeframes

The primary objective of Article 34 GDPR is to equip data subjects with the necessary safeguards against further adverse consequences of a breach.[202] Whether this effectively contributes to the reduction of risk and the implementation of protective measures depends on different factors. Effective communication requires the use of transparent sources (like direct messaging, prominent website banners and printed advertisements, or postal communication) and easily understandable language.[203] Controllers can also offer data subjects specific guidance on what steps to take to protect themselves.[204] Depending on the circumstances of the breach, these may include changing passwords, implementing security measures, securing accounts with financial institutions or other organizations, requesting credit reports and obtaining credit report bans against third parties.[205] The timing of the communication is

[201] Indeed, during this crucial time (research mode phase 2) entities need to gather as much as possible information on the incident and analyze it. See: Sandra Schmitz and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 101, 109. The incident handling phases are explained by: Paul Cichonski et al, 'Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology' (NIST National Institute of Standards and Technology, 2012) https://rms.koenig-solutions.com/Sync_data/Trainer/QMS1784-2020417482-NIST.SP.80061r2.pdf accessed last 1 June 2023

[202] Mario Renna, 'Data Breach Disclosure Duties' (2019) 2 European Journal of Privacy Law & Technologies 2 (2019) 79, 82-83; Mark Verstraete and Tal Zarsky, 'Optimizing Breach Notification' (2020) 2021 University of Illinois Law Review 803, 818; Mehmet Bedii Kaya, 'Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law' (2021) 70 Annales de la Faculté de Droit d'Istanbul 195, 211

[203] Mario Renna, 'Data Breach Disclosure Duties' (2019) 2 European Journal of Privacy Law & Technologies 2 (2019) 79, 85; European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 21

[204] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 21

[205] Dennis Gibson, Clive Harfield 'Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy' (2022) 29:7 International Review of Victimology 1, 7

important to ensure that data subjects have the necessary time and opportunity to react.[206] Therefore, communication must be done without delay. Differently, NIS2 Article 23 aims to reinstate information security networks and systems.[207] Immediate notification and public disclosure of significant incidents could impair that, conflicting with NIS2 objectives.[208] In some cases, a GDPR breach also constituting a NIS2 incident might necessitate delayed communication to data subjects. This complicates compliance, as an entity cannot avoid immediate public notification under a NIS2 perspective without failing to comply with GDPR as a controller in case the data breach is likely to present high-risk for data subjects.

Importantly, these differing obligations rests on the notion of 'undue delay', which impacts the timeframes that entities and controllers must abide by for compliance. Undue delay's interpretation is not uniform across GDPR. For instance, in the context of the exercise of data subjects' rights, it is interpreted as one month at the latest with a possible extension of two further months if necessary, based on the complexity and the number of requests received by one controller.[209] Similarly, regarding mutual assistance between supervisory authorities, undue delay is interpreted as no later than one month from the request.[210] Moreover, given the GDPR's risk-based approach, interpretation should account for the context of a specific breach: severity, affected individuals, breach awareness, complexity, and mitigation measures should all be taken into account. Compliance should be also contextual and driven by risk analysis.[211] Under Article 34 GDPR, depending on the interpretation of undue delay controllers may have a shorter or longer, specific or flexible timeframe during which notification and publicity of the incident can be delayed for information security reasons.

The concern arises that when premature, public communication of an incident might harm information security and NIS2 objectives.[212] Data subject notification often results in broader public disclosure, requiring entities to go public on the incident.[213] Schmitz-Berndt's

[206] Mario Renna, 'Data Breach Disclosure Duties' (2019) 2 European Journal of Privacy Law & Technologies 2 (2019) 79, 81
[207] Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 453
[208] Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 449
[209] Article 12 (3) GDPR
[210] Article 61 GDPR
[211] Rita Heimes, 'Global InfoSec and Breach Standards' (2016) 14:5 IEEE Security & Privacy 68, 68-69
[212] Karen Mc Cullagh, Kim Barker and Gavin Sutter, 'Regulating transitions in technology, law, and beyond' (2021) 35:2 International Review of Law, Computers & Technology 99, 99
[213] Karen Mc Cullagh, Kim Barker and Gavin Sutter, 'Regulating transitions in technology, law, and beyond' (2021) 35:2 International Review of Law, Computers & Technology 99, 99

work is the main source of literature on the relationship between the two NIS1/2 and GDPR's notification frameworks and the concern parallel compliance could result in premature public disclosure, as a consequence of the immediate notification to the data subject, thereby undermining NIS2.

4.2. Premature Public Disclosure and Reasons for Delayed Disclosure

Avoiding premature public disclosure, by delaying immediate data subject notification under Article 34 GDPR, is argued to be necessary not to jeopardize efficient incident response under NIS2. Oftentimes notification to the data subjects results in broader public disclosure and forces an entity to go public on the incident.[214] While Schmitz's argument refers specifically to the interplay between GDPR and NIS1, it forms part of a larger discourse on vulnerability disclosure and its potentially harmful effects on cybersecurity. This discussion generally rests on the trade-off between the benefits and costs of disclosure and its timing.[215]

The underlying challenge is designing disclosure in a way that yields net positive outcomes.[216] In the NIS2-GPDR dynamics, the aim is striking a balance (in terms of both content and time) where disclosure facilitates timely data subject notification, so they can protect themselves while avoiding revealing information that could be exploited by attackers. Indeed, entities have reasons to delay the notification of individuals under Article 34 GDPR considered the incident response cycle by NIST.[217] During the detection and analysis phase of an incident, entities must gather and examine comprehensive amounts of data. Premature disclosure at this stage could interfere with subsequent containment and recovery efforts,

---

[214] Karen Mc Cullagh, Kim Barker and Gavin Sutter, 'Regulating transitions in technology, law, and beyond' (2021) 35:2 International Review of Law, Computers & Technology 99, 99, Sandra Schmitz and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 106-107

[215] Holly Stewart and Tom Cross, 'Lessons learned: can alerting the public about exploitation do more harm than good?' (Virus Bulletin Conference, 2013) https://www.virusbulletin.com/files/StewartCross-VB2013.pdf last accessed 8 August 2023, 58; Roland L Trope and Sarah Jane Hughes, 'The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-thieves More?' (2011) 1 Business Law Today, 1
Holly Stewart and Tom Cross, 'Lessons learned: can alerting the public about exploitation do more harm than good?' (Virus Bulletin Conference, 2013) https://www.virusbulletin.com/files/StewartCross-VB2013.pdf last accessed 8 August 2023, 58

[216] Holly Stewart and Tom Cross, 'Lessons learned: can alerting the public about exploitation do more harm than good?' (Virus Bulletin Conference, 2013) https://www.virusbulletin.com/files/StewartCross-VB2013.pdf last accessed 8 August 2023, 58

[217] Sandra Schmitz and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 101, 106-109

jeopardizing the overall NIS2's aim of restoration of the security system.[218] There are several reasons for this. Firstly, premature disclosure can interfere with the identification of attackers and weaken efforts to monitor their techniques and communication methods.[219] Early disclosure might alert attackers to the detection of the incident, causing them to shift their attack vector and strategy.[220] Secondly, other malicious actors might capitalize on the disclosed vulnerability, potentially leading to further attacks.[221] Empirical evidence suggests that hackers closely follow current vulnerabilities, and tend to target those that have been already successfully exploited.[222] This indicates the potential value and effectiveness of targeting those vulnerabilities, serving as a blueprint for ulterior attacks.[223] Although there might be also individualistic reasons for entities to avoid/delay disclosure, such as reputational loss, these secondary motives are not discussed here.[224] This thesis focuses on the technical reasons warranting a delayed public communication for information security considerations of significant incidents which are also personal data breaches.

The EDPB provided two relevant examples of harm arising from premature public disclosure.[225] Instances like ransomware attacks, as evidenced by the NHS attack in 2017, and data infiltration attacks are scenarios where this conflict is likely to rise.[226] In ransomware attacks, public communication might be harmful where a severe interruption of service and sensitive personal data is involved.[227] Beyond the direct consequences of the attack, the vast spread of malware contributes to the high number of unpatched systems, particularly those hard

---

[218] Ibid 107-109

[219] ibid

[220] Ibid

[221] Jay P Kesan and Carol Mullins Hayes, ''Bugs in the market: creating a legitimate, transparent, and Vendor-Focused Market for Software Vulnerabilities' (2016) 58 Arizona Law Review 753, 794

[222] Ibid 794-795

[223] Christina Parajon Skinner, 'Bank Disclosures of Cyber Exposure' (2019) 105 Iowa Law Review 239, 273

[224] Marleen Weulen Kranenbarg, Thomas J. Holt and Jeroen van der Ham, 'Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure' (2018) 7:16 Crime Science 1, 4

[225] European Data Protection Board, 'Guidelines 01/2021 on examples regarding data breach notification' (EDPB, 14 January 2021) https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf last accessed 8 August 2023, 11-12

[226] European Data Protection Board, 'Guidelines 01/2021 on examples regarding data breach notification' (EDPB, 14 January 2021) https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf last accessed 8 August 2023, 7; Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 451-453

[227] Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 451-453

to patch due to legacy support systems. In these cases, immediate publicity should be avoided: in order to prevent compromising further personal data, disclosure should be postponed until after the release of a patch for the software vulnerability.

4.3. Undue Delay under GDPR

Data subjects notification must be made without undue delay. Unlike the notification to the DPAs, under Article 34 GDPR there is no precise time limit.[228] This lack of definition has been reflected by the different interpretations among Member States.[229] Recital 86 GDPR interprets it as 'as soon as reasonably feasible'.[230] However, it also acknowledges the possibility of justified delayed disclosure. For example, a delay may be justified when needed to implement appropriate measures against continuing or similar personal data breaches.[231] Therefore, in principle, GDPR recognizes possible reasons for delay.[232] However, this potential extension appears closely constrained in practice, due to the lack of specifications by the legislator.[233]

Indeed, the term "may" implies that delay can be granted only in some cases, without however specifying how to ascertain when the implementation of appropriate measures against continuing or similar breaches is needed. Moreover, Recital 86 only refers to continuing attacks, without indicating how to distinguish them from terminated ones. This raises questions on whether delay could apply to cases where the data breach is terminated (not ongoing) but the security vulnerabilities (linked to the security incident and the NIS2 relevant aspect of the event) are continuing. Schmitz's argument emphasizes that Recital 86 does not address explicitly ongoing security incidents, therefore leading to the conclusion that it only allows for suggests justified delayed disclosure for a few, yet not clearly specified grounds.[234] Seemingly,

---

[228] Article 33 GDPR

[229] Conseil des barreaux européens, 'CCBE Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR)' (CCBE, 19 May 2017) https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf accessed 1 June 2021, 2

[230] Recital 86 GDPR

[231] Recital 86 GDPR in conjunction with Art 34(2); Anneliese Roos, 'Data Protection Principles under the GDPR and the POPI Act: A Comparison' (2023) 86:1 THRHR 1, 18

[232] Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 452

[233] Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 452

[234] Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 452

significant incidents incidentally involving personal data breaches but giving rise to an ongoing targeted attack at other vital systems of the entities are excluded, to the detriment of NIS2's considerations.

Additional guidance on the interpretation of undue delay is provided by WP29 and the EDPB.[235] However, clearer instructions should be provided on the circumstances under which justified delay can be awarded. Currently, justified delayed is specified only in the interests of law-enforcement authorities.[236] On the other hand, cases where private entities face reporting obligations on their own with the reporting obligations, remain unclear. [237] Fangei Wang's analysis of undue delay under the revised e-Privacy Directive underscores its importance to ensure timely and certainty of data protection.[238] Wang criticizes the ambiguous legal terms and threshold for notification of personal data breaches, advocating for clearer criteria that can be better integrated into business models and technical calculations.[239] Clear and transparent exceptions to the strict timeframes of notification requirements are needed, taking into consideration situations where disclosing information may harm prioritizing system integrity

[235] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (Article 29 WP, February 2018) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiH06aVuvz9AhVbhf0HHTchAK0QFnoECA0QAQ&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fredirection%2Fdocument%2F51025&usg=AOvVaw1ZPWgd7ZxqhDx-kJK5DxmF> last accessed 8 August 2023; European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 8 August 2023, 19-22.

[236] Recital 88 GDPR

[237] Sandra Schmitz and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal' 12 (2021) JIPITEC 448, 452; Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (Article 29 WP, February 2018) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiH06aVuvz9AhVbhf0HHTchAK0QFnoECA0QAQ&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fredirection%2Fdocument%2F51025&usg=AOvVaw1ZPWgd7ZxqhDx-kJK5DxmF> last August 2023, 21

Conseil des barreaux européens, 'CCBE Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR)' (CCBE, 19 May 2017) 1-2 https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf; Article 70 GDPR

[238] Faye Fangfei Wang, 'Personal Data Breach Notification System in the European Union: Interpretation of "Without Undue Delay"' (2011) 22:6 European Business Law Review 741, 751

[239] ibid

restoration or investigation. [240] This closely resembles the criticism moved against "undue delay" under GDPR.

Factors influencing undue delay include the timing of breach awareness, the specific circumstances, and the effectiveness of the security system. The timing of notification begins with the controller's awareness of the data breach, which starts when there is reasonable certainty of a breach compromising personal data.[241] Controllers must act promptly to determine the breach and exercise diligence. [242] This includes technical and organizational measures to detect the breach and perform notification duties.[243] Proper diligence and compliance must be demonstrable throughout accountability and the documentation of the development of the breach.[244] Effective internal processes, detection and alert mechanisms should be established.[245] They include data flows and log analysers to facilitate the definition of events and traceability of how personal data has been processed so that controllers can better identify and trace back potential breaches.[246] Secondly, the specific circumstances of the breach also impact the timing.[247] While some breaches are immediately apparent, others require further investigation. The ultimate goal is to promptly identify data breaches and remedy them, and notify data subjects if required.[248] The threshold for notification, in this regard, is determined in accordance with the merits of the breach, the type of the data (e.g. sensitive data),

---

[240] František Kasl, 'The US Lessons for the EU Personal Data Breach Notification: Part II – The EU Regulatory Perspective and Discussion of the Benefits Available from the US Experience' 11:1 (2021) The Lawyer Quarterly 192, 203

[241] Mario Renna, 'Data Breach Disclosure Duties' (2019) 2 EUR. J. PRIVACY L. & TECH. 79, 84

[242] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 11-13

[243] GDPR Art. 32

[244] This is in line with the principle of accountability and the obligation to record personal data processing activities, see Arts. 5(2) and 30 GDPR

[245] European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 12

[246] Andrew Brown, 'GDPR compliance and log data' (NXLOG, 23 September 2022) https://nxlog.co/news-and-blog/posts/gdpr-compliance last accessed 8 August 2023;
Darko Samardžić, 'Records of processing activities (Art. 30 GDPR) in analogue and digital ecosystems' (2021) 14 ANALI Pravnog Fakulteta Univerziteta U Zenici 183, 186

[247] Irish Data Protection Commission, 'A Practical Guide to Personal Data Breach Notifications under the GDPR' (Data Protection Commission, October 2019), https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf last accessed 10 August 2023, 13

[248] Mario Renna, 'Data Breach Disclosure Duties' (2019) 2 European Journal of Privacy Law & Technologies 2 (2019) 79, 85-86

and the severity of the breach.[249] Finally, the overarching security system structure must be considered. Open communication between all involved actors (controller, processor, data subject, competent authority) is necessary for efficient preventive relief and remedial measures to the data breach.[250] Throughout this assessment, the paramount goal of the response plan from a GDPR standpoint is the protection of individuals and their personal data.

4.4. Undue delay under NIS2

The NIS1 framework will also be described, as it serves as the context within which the issue of premature disclosure first emerged. The absence of a definition of "undue delay" under NIS1 was both surprising and problematic, given that it was the only temporal reference for reporting obligations.[251] Consequently, various interpretations emerged among Member States, which ranged from 'immediately', to 'within 24 hours' or even longer timeframes.[252] The lack of guidance led to criticism, amid insufficient reporting and information sharing.[253] However, NIS2 did address the potential extension of undue delay under certain circumstances: Recital 59 NIS1 acknowledged the possible suspension of public notification, provided that the interests of both the public and of the entities would be considered.[254] Furthermore, it required competent authorities and CSIRTs to maintain strict confidentiality on information on product vulnerabilities until the release of appropriate security fixtures.[255] Thus, Recital 59 NIS1 allowed for the delayed disclosure of an incident until adequate protective measures would be

[249] Mehmet Bedii Kaya, 'Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law' (2021) 70 Annales de la Faculté de Droit d'Istanbul 195, 211

[250] Recital 86 GDPR; Mario Renna, 'Data Breach Disclosure Duties' (2019) 2 European Journal of Privacy Law & Technologies 2 (2019) 79, 84

European Data Protection Board, 'Guidelines 9/2022 on personal data breach notification under GDPR' (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf last accessed 1 March 2022, 20

[251] Articles 14(3) and 16 NIS1

[252] Sandra Schmitz-Berndt, 'Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes' in Cyril Onwubiko, Pierangelo Rosati, Aunshul Rege et als (eds), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (Springer Singapore 2023) 343, 345

[253] Sandra Schmitz-Berndt, 'Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes' in Cyril Onwubiko, Pierangelo Rosati, Aunshul Rege et als (eds), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (Springer Singapore 2023) 343, 345

[254] Recital 59 NIS1

[255] Ibid

available.[256] Therefore, Recital 59 NIS1 seemed to conflict with Article 34 and Recital 86 GDPR and the immediate notification of data subjects.[257]

While NIS2 also does not define how "undue delay" should be interpreted, it does significantly revise reporting obligations, influencing their interplay with GDPR in terms of easing compliance and concern about premature disclosure. The updated NIS2 framework introduces a tiered notification plan which incorporates specific deadlines and timeframes.[258] This change might account for the lack of guidance on precise undue delay interpretation, as now clearer and structured timelines are also provided. Similar to GDPR, timing starts running upon the entity's awareness of the incident.[259] This reduces the fragmentation caused by NIS1's broad discretion and increases harmonization.

Unlike NIS1, which presented no obligation for general public disclosure of incidents, NIS2 requires entities to notify, without undue delay, the recipients of their services of significant incidents likely to adversely impact the provision of those services.[260] This first change brings NIS2 closer to the GDPR than under NIS1, where public disclosure did not amount to an obligation and necessitated balancing the interests of the public in being informed and those of the reporting entities.[261] This development bridges the gap between Article 34 GDPR's requirement to notify data subjects without undue delay, and the absence of such disclosure provision under NIS1. While these amendments are expected to enhance reporting practices and harmonization, the potential for differences in timeframes between NIS2 and GDPR to cause premature disclosure is not directly addressed. While NIS1 Recital 59 explicitly recognized that there may be reasons for delaying public disclosure of an incident, NIS2 lacks an analogous provision. Indeed, there is no reference to the possibility of justified delayed notification. NIS2 does not contain any reference to the possibility of extending undue delay.

4.5. Synergies Between NIS2 and GDPR

Exploiting synergies of different EU reporting obligation schemes, including NIS1 and GDPR is a suggested approach by the NIS Cooperation Group. Improved synergies would

[256] Recital 59 NIS1

[257] Sandra Schmitz and Stefan Schiffner, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 101, 109

[258] As presented in Chapter 3

[259] Philipp Eckhardt and Anastasia Kotovskaia, 'The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive' (2023) 4 International Cybersecurity Law Review 147, 159

[260] Article 23(1) NIS2

[261] Recital 59 and Article 14(6) NIS1

facilitate compliance with these co-existing frameworks and could ease the concern over premature public disclosure. NIS2 brings changes that match some of the findings of the NIS Cooperation Group, particularly the alignment/harmonization of existing reporting schemes, both at the national and European levels. Under NIS2 the competent authorities/CSIRTs will provide, without undue delay and where possible within 24 hours from the early warning receipt, a response to the notifying entity, which must include initial feedback.[262] CSIRTs will assume more important roles, carrying out incident response tasks, facilitating national and international cooperation, and providing assistance to entities, and potentially guiding them on the notification of significant incidents involving a personal data breach.[263]

Moreover, NIS2 fosters formal cooperation and exchange of information between GDPR and NIS2 authorities. In particular, it mandates cooperation with the relevant authorities when personal data are breached during a significant incident.[264] This emphasis will benefit information sharing and improve the synergies between the two frameworks. Therefore, all these NIS2 changes bring greater structure and clarity to the notification and handling of significant incidents, mitigating concerns about the lack of guidance on undue delay.

Nevertheless, it is worth noting that NIS2 as a Directive, requires Member States to transpose it to their national legal systems.[265] The deadline is set on 17 October 2024.[266] While adopting measures to transpose NIS2 under their domestic laws, Member States must achieve the objectives set by NIS2. Under EU law, through Directives Member States are awarded with some discretion as to how these objectives should be achieved.[267] This is significant, overall for the effectiveness of NIS2 and more specifically for the subject of this research, as reporting obligations and the above-mentioned NIS2 changes will be to some extent also depend on the national implementation of the Directive.[268] One major cause of weakness for NIS1 was the

[262] Article 23(5) NIS2
[263] Article 11 NIS2
[264] Article 31(3) NIS2
[265] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU), Article 288
[266] Article 41 NIS2
[267] European Parliament Research Service, 'Transposition, implementation and enforcement of Union law' (EPRS, November 2018) https://www.europarl.europa.eu/cmsdata/226403/EPRS_ATAG_627141_Transposition_implementation_and_enforcement_of_EU_law-FINAL.pdf accessed 20 August 2023
[268] Theodoros Karathanasis, 'Member States Confronted with EU-Based Rules in the Field of Cybersecurity, The Effectiveness of Directive (EU) 2016/1148' (Phd Thesis, Université Grenoble Alpes 2022) https://theses.hal.science/tel-04077226v1/file/KARATHANASIS_2022_archivage.pdf accessed 20 August 2023, 30-31

broad discretion that it left to Member States.[269] Noteworthy, the more precise and direct language of NIS2 reduces this discretionary gap.[270] Concerning the reporting obligations, Article 23 NIS2 presents a more structured and complete set of obligations than Articles 14 and 16 NIS1. As a result, it can be expected that the divergencies between different Member States' implementation will also be reduced compared to NIS1.[271]

4.6. Contextualizing the Conflict under EU Law

While changes brought by NIS2 harmonize and facilitate reporting of significant incidents, as well as align and bridge some of the gaps between reporting systems under NIS2 and GDPR, they do not address the issue of premature public disclosure as such. In this context, coming up with an approach to address this potential conflict by way of establishing precedence between NIS2 and GDPR could be useful. While NIS1 and GDPR did not explicitly acknowledge each other, now NIS2 references the GDPR and mandates its application without prejudice to the latter.[272] While their interaction in terms of reporting obligations has been discussed in the previous chapter, Markopoulou discusses their interplay and their potential conflicts with a broader view.[273] On the relationship between reporting obligations, Markopoulou offers a similar conclusion to Chapter 3, asserting that incidents qualifying as both personal data breaches and significant incidents should be assessed and reported independently under NIS2 and GDPR, due to the different scopes of these instruments.[274]

However, Markopoulou adds to the discussion by arguing that in any cases of conflict between the two, GDPR should take precedence.[275] The reasons are twofold. First, based on the status of the right of data protection as a fundamental EU right based on Article 16(2) TFEU.[276] This makes data protection a horizontal legal obligation under EU law, whose respect and exercise would take precedence over cybersecurity.[277] Secondly, given the relationship

[269] Valentino Lucini, 'The ever-increasing cybersecurity compliance in Europe: the NIS2 and what all businesses in the EU should be aware of' (2023) 11 Russian Law Journal 145, 146
[270] Niels Vandezande, 'Cybsersecurity in the EU: how the NIS2-Directive stacks up against its predecessor' (KU Leuven - Centre for IT & IP Law, 2023) https://ssrn.com/abstract=4383118 last accessed 10 August 2023, 7
[271] Ibid
[272] Recitals 14 and 92, Article 2(12) NIS2
[273] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review, 10-11
[274] Ibid
[275] Ibid
[276] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU), Article 16(2)
[277] Ibid

between NIS2 and GDPR based on their nature of Directive and Regulation. Indeed, NIS2 is a Directive, which must be transposed into national law by Member States.[278] GDPR, as a Regulation, has been directly applicable into the domestic legal systems of Member States.[279] Would conflict arise between GDPR and the nationally implemented NIS2, the former would prevail given that EU law has precedence over Member State law.

This approach suggests examining the protection goals of NIS2 and GDPR, along with their nature as regulatory frameworks. Noteworthy, they protect different interests: data protection rights concerning personal data of individuals under GDPR and cybersecurity under NIS2. This distinction provides valuable insight into their relationship. This has been used to better understand their coexistence and their application, as shown throughout the previous Chapters.[280] Based on these insights, design choices of different timelines in the reporting obligations and interpretation of undue delay can be appreciated. Although Markopoulou does not explicitly cover this aspect, the suggested is still used to infer a hierarchical relationship in case of conflict. This may offer a possible answer to whether priority should be given to the notification without delay to data subjects under Art. 34 GDPR, based on its overarching priority over NIS2. While this would not solve the concerns about premature disclosure, establishing a prevalence between the application of the two legal instruments would increase legal certainty for entities on how to secure compliance in cases where a personal data breach also amounts to a significant incident.

4.7. Conclusion

The different timelines, especially in relation to the interpretation of 'undue delay', between NIS2 and GDPR might give rise to premature public disclosure of significant incidents, thereby jeopardizing incident response. However, these differences can be explained by the different protection goals of the NIS2 and GDPR, which could also be ultimately used to establish prevalence and prioritize data protection and the GDPR when compliance under both is requested. Moreover, the potential of premature disclosure has been argued in relation to NIS2, and this thesis aims at re-contextualizing this issue in the framework of NIS2. While

[278] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU), Article 288
[279] Ibid
[280] Paula Contreras, *The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges* (International Conference on Cybersecurity, Situational Awareness and Social Media, Wales, 2022) https://link.springer.com/chapter/10.1007/978-981-19-6414-5_18 327, 335

the changes under NIS2 do not directly address premature disclosure they improve the reporting system and allow for better synergies and stronger cooperation between authorities.

Chapter 5 – Conclusion

Cybersecurity currently faces a rising volume of attacks, many of which involve personal data breaches. The importance of a harmonized and stronger cybersecurity framework was emphasized by the COVID-19 pandemic, which heightened society's increasing reliance on ICT services underpinning the operations of critical network and information systems.[281] Set against this background and aiming to enhance the flawed predecessor, the EU adopted the NIS2 which will have to be transposed by Member States by October 2024. Under NIS2, a key goal is the streamlining of incident reporting obligations: an efficient notification system is crucial, with a broader view of increasing cyber-resilience within the context of the internal market.[282] However, the NIS2 reporting system intersects with that established by the GDPR. While they have different objectives, formats and timeframes, their interaction is worth investigating since information security breaches often involve personal data. Noteworthy, often the same event qualifies as both a personal data breach and a significant incident, and notification will be performed under NIS2 by essential and important entities, which also frequently act as controllers, joint controllers, and processors under GDPR. This significant overlap in the application of both frameworks and the relevant notifying actors raises the question of whether the same event must be notified under both NIS2 and GDPR and the implications thereof. This thesis aims to answer the main research question: "What is the relationship between the parallel mandatory reporting obligations of NIS2 and GDPR and how is this affected by their different timelines in light of premature public disclosure?".

To answer this, mostly comparative legal research was conducted, relying on primary and secondary sources. Initially, the mandatory notifiable incidents under NIS2 and GDPR were described and compared, along with their respective notifying entities and authorities. Chapter 3 examines and compares the procedural aspects of the reporting obligations as provided by Articles 23 NIS2 and 33-34 GDPR. Their different timelines, whose design is crucial to ensure entities and data controllers require sufficient time for effective compliance, are a particular point of contention. It is at this juncture that the potential issue of premature public disclosure comes into play, as investigated in Chapter 4. In cases where a data breach

[281] Niels Vandezande, 'Cybsersecurity in the EU: how the NIS2-Directive stacks up against its predecessor' (KU Leuven - Centre for IT & IP Law, 2023) https://ssrn.com/abstract=4383118 last accessed 10 August 2023, 3-4

[282] Dimitrios D Skias et al, 'Demonstration of alignment of the Pan-European Cybersecurity Incidents Information Sharing Platform to Cybersecurity policy, regulatory and legislative advancements' (17th International Conference on Availability, Reliability and Security ARES, New York, 2022) https://dl.acm.org/doi/pdf/10.1145/3538969.3544477, 2

also qualifies as a significant incident, immediate notification to data subjects has been argued to potentially result in premature public disclosure, undermining the protection goals of NIS2. This required examining the interpretation of 'undue delay' under NIS2 and GDPR. An analysis of Article 34 in conjunction with Recital 86 GDPR suggests that a delayed disclosure is not justified for ongoing significant incidents that involve a terminated personal data breach, and for which public enforcement authorities are not involved. Therefore, to be GDPR-compliant, controllers need to perform immediate notification, to the potential detriment of NIS2 due to the premature disclosure. The concern for premature public disclosure finds support in the broader discussion on vulnerability disclosure, although there are very few sources specifically addressing the NIS1/2-GDPR case, apart from Schmitz. Nevertheless, considering that NIS2 has introduced significant changes to the overall Directive, particularly to its reporting obligations, the potential issue of early public disclosure needs to be re-evaluated in light of the new NIS2 framework. This thesis addresses that, by incorporating these developments to reframe the existing discussion.

Recipients of services, whose provisions are likely to be adversely affected by significant incidents, are now also notified under NIS2 without undue delay. This change brings the reporting schemes of NIS2 and GDPR closer together, as it requires immediate broader disclosure, aligning with the obligation of notifying data subjects under Article 34 GDPR. Additionally, the NIS2 three-tiered notification plan introduces specific deadlines and timeframes that reduce fragmentation and involve competent authorities and CSIRTs more actively. Their response and feedback will better guide entities in complying with reporting obligations and incident handling. These changes reflect NIS2's clear intention to increase overall information sharing and are part of a broader positive development that promotes extended reporting and cooperation between authorities. In fact, NIS2 may strengthen the cooperation between national competent authorities and data protection authorities. While not examined in detail due to word count limitations, this notable change will benefit the notification systems of both GDPR and NIS2.

However, to the best of my knowledge, there is an insufficient amount of evidence of cases where immediate notification of data subjects caused premature public disclosure and explicitly harmed an entity's containment and recovery efforts. This limited the use of specific cases and incident reports, and represented the main limitation of this research, which remained extensively theoretical and lacked the empirical resources to appreciate and evaluate premature disclosure from a more practical viewpoint. In particular, the degree of leverage that can be gained by malicious actors through data-subject communication should be further researched.

There is a risk, acknowledged by Schmitz herself, that this could be overestimated.[283] However, this does not diminish the significant overlap and interaction points between NIS2 and GDPR, among which parallel notification obligations are recognized as contentious. Notably, it has been argued that in cases of conflicting obligations between NIS2 and GDPR, the latter should take precedence. Markopoulou et al argue that, based on its status as a fundamental EU right, data protection should be prioritized over cybersecurity.[284] Furthermore, the nature of the GDPR as an EU Regulation would prevail over NIS2, which -being a Directive- is implemented as domestic law.[285] Applied to the context of premature public disclosure, this suggests that the rights of data subjects should prevail.

In conclusion, the concern regarding premature public disclosure is alleviated by the amendments introduced by NIS2, which align its provisions more closely with GDPR. This aligns with the suggestion of the NIS Cooperation Group, which analyzed cybersecurity incident reporting and encouraged increased harmonization as a facilitator for compliance and effective incident handling.[286] However, further guidance on the possibility of delayed disclosure to data subjects would still be welcomed. As it currently stands, Recital 86 GDPR does not provide sufficient clarity regarding its applicability to data breaches that also qualify as significant incidents under NIS2. Detailed guidance would clarify whether delayed disclosure beyond undue delay is permissible in cases where it aids in the containment and recovery of the incident, similar to how Recital 88 GDPR addresses the interests of law enforcement. Once NIS2 will be transposed by the Member States and enter into force, practice will show whether the concurrent reporting duties will be sufficiently streamlined or might lead to premature disclosure of significant incidents. This is especially interesting given the expected increase in reporting obligations as linked to the extended scope of NIS2.

[283] Sandra Schmitz-Berndt and Stefan Schiffner, 'Responsible vulnerability disclosure under the NIS 2.0 Proposal, Interplay of the Reporting Schemes and the Potential Risk of Early Vulnerability' (2021) 12 JIPITEC 447, 453

[284] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 1, 10-11

[285] ibid

[286] NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting' (CG Publication, April 2020) <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group> last accessed 13 July 2023

BIBLIOGRAPHY

Primary sources:

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU)

Council of Europe, Convention on Cybercrime of 23 November 2001, <https://www.refworld.org/docid/47fdfb202.html> accessed 8 August 2023

Council of the European Union, 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 2016/1148 (17 June 2022) <https://data.consilium.europa.eu/doc/document/ST-10356-2022-INIT/en/pdf> accessed 8 August 2023

Council Regulation (EC) 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency [2004] *OJ L 77/1*

Directive (EU) 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337/11

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80

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 [2016] OJ L 119/1.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and

communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L 151/15

Secondary Sources

Alunge R, 'Breach of security vs personal data breach: effect on EU data subject notification requirements' (2021) 11 International Data Privacy Law

Andreasson A and Fallen N, 'External Cybersecurity Incident Reporting for Resilience' in J Zdravkovic et al (eds), *Perspectives in Business Informatics Research* (Springer Cham 2018)

Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679' (Article 29 WP, February 2018) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiH06aVuvz9AhVbhf0HHTchAK0QFnoECA0QAQ&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fredirection%2Fdocument%2F51025&usg=AOvVaw1ZPWgd7ZxqhDx-kJK5DxmF> accessed 8 August 2023

Ayyagari R, 'Data breaches and Carding' in Thomas J Holt and Adam M Bossler (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Palgrave Macmillan 2020)

Bederna Z and Rajnai Z, 'Analysis of the cybersecurity ecosystem in the European Union' (2022) 3 Int. Cybersecur. Law Rev

Bisogni F, Asghari H and van Eeten M, '*Estimating the size of the iceberg from its tip: An investigation into unreported data breach notifications'* (Proceedings of 16th Annual Workshop on the Economics of Information Security, La Jolla, 2017) <https://pure.tudelft.nl/ws/portalfiles/portal/28437304/WEIS_2017_paper_54_2.pdf> accessed 8 August 2023

Bitkom, 'Bitkom position on the proposal for a renewed Directive on security of network and information systems' (*Bitkom, March 2021*) <https://www.bitkom.org/sites/default/files/2021-03/210318_pp_nis-directive-2.pdf> accessed 8 August 2023

Bitkom, 'NIS Directive 2.0 – Bitkom Position' Bitkom position on the proposal for a renewed Directive on security of network and information systems' (Bitkom, 3 January 2022) https://www.bitkom.org/sites/default/files/2022-01/03.01.22_bitkom_nis2_positionspapiertrilog.pdf

Brighi R and Chiara PG, 'La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea' (2021) 21 Federalismi.it

Brown A, 'GDPR compliance and log data' (NXLOG, 23 September 2022) https://nxlog.co/news-and-blog/posts/gdpr-compliance accessed 8 August 2023

Chiara PG, 'The IoT and the new EU cybersecurity regulatory landscape' (2022) 36:2 International Review of Law, Computers & Technology

Cichonski P et al, 'Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology' (NIST National Institute of Standards and Technology, 2012) https://rms.koenig-solutions.com/Sync_data/Trainer/QMS1784-2020417482-NIST.SP.80061r2.pdf accessed 8 August 2023

Contreras P, *The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges* (International Conference on Cybersecurity, Situational Awareness and Social Media, Wales, 2022) https://link.springer.com/chapter/10.1007/978-981-19-6414-5_18

Cormack A, 'NISD2: A Common Framework for Information Sharing among Network Defenders' (2021) 18 SCRIPTed 83

Conseil des barreaux européens, 'CCBE Guidance on the main new compliance measures for lawyers regarding the General Data Protection Regulation (GDPR)' (CCBE, 19 May 2017) https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf accessed 8 August 2023

Council of the European Union, 'Press Release - Strengthening EU-wide cybersecurity and resilience – provisional agreement by the Council and the European Parliament' *(Council of the European Union, 13 May 2022)* <https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/> accessed 8 August 2023

Cyentia, 'Information Risk Insights Study (IRIS) Tsunami – Following the wake of damage from major multi-party cyber incidents' (Cyentia, 2021) https://www.cyentia.com/wp-content/uploads/IRIS-Tsunami.pdf accessed 20 August 2023, 17

Daigle B and Khan M, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' (2020) Journal of International Commerce and Economics

Del Mar M and Negreiro A, 'ENISA and a new cybersecurity act' *(European Parliamentary Research Service, July 2019)* <https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf> accessed 8 August 2023

Del Mar M and Negreiro A, 'The NIS2 Directive - A high common level of cybersecurity in the EU' *(The NIS2 Directive - A high common level of cybersecurity in the EU, June 2022)* <https://www.europarl.europa.eu/thinktank/nl/document/EPRS_BRI(2021)689333> accessed 8 August 2023

Digital Europe, 'Harmonising cyber protection across Europe: The digital industry's basic asks for the NIS2 trilogues' (*Digital Europe, February 2022)* <https://www.digitaleurope.org/resources/harmonising-cyber-protection-across-europe-the-digital-industrys-basic-asks-for-the-nis2-trilogues/> accessed 8 August 2023

Drivas G and others, 'A NIS Directive Compliant Cybersecurity Maturity Assessment Framework' (2020) IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)

Eckhardt P and Kotovskaia A, 'The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive' (2023) 4 International Cybersecurity Law Review

ENISA, 'Coordinated Vulnerability Disclosure policies in the EU' *(ENISA, April 2022)* < https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu> accessed 8 August 2023

European Banking Foundation, 'EBF key messages on the proposal for a Revised Directive on Security of Network and Information Systems (NIS2)' *(EBF, June 2021)* <https://www.ebf.eu/wp-content/uploads/2021/06/EBF-key-messages-on-NIS2-proposal.pdf> accessed 8 August 2023

European Commission, 'Impact Assessment Report accompanying the document 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' (*European Commission, 16 December 2020)* 345 final, part 1/3

https://ec.europa.eu/newsroom/dae/redirection/document/72176 accessed 20 August 2023

European Commission, 'Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)' (*European Commission, January 2021*) <https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1/language-en> accessed 8 August 2023

European Cyber Security Organisation, 'Position Paper on the NIS Directive Review' *(ECS, November 2020)* < https://ecs-org.eu/wp-content/uploads/2022/10/5fd24425bc74c.pdf> accessed 8 August 2023

European Data Protection Board, *Guidelines 9/2022 on personal data breach notification under GDPR* (EDPB, 10 October 2022) https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf accessed 8 August 2023

European Data Protection Board, *Guidelines 7/2020 on the concepts of controller and processor in the GDPR* (EDPB, 07 July 2021) https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf accessed 8 August 2023

European Data Protection Supervisor 'Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive' *(EDPS, 11 March 2021)* <https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf> accessed 8 August 2023

European Parliament Research Service, 'Transposition, implementation and enforcement of Union law' (EPRS, November 2018) https://www.europarl.europa.eu/cmsdata/226403/EPRS_ATAG_627141_Transposition_implementation_and_enforcement_of_EU_law-FINAL.pdf accessed 20 August 2023

Gabel D and Hickman T, 'Chapter 14: Data Protection Authorities – Unlocking the EU General Data Protection Regulation' (White & Case, 5 April 2019) https://www.whitecase.com/insight-our-thinking/chapter-14-data-protection-authorities-unlocking-eu-general-data-protection accessed 17 August 2023

Gibson D, 'Amplifying victim vulnerability: Unanticipated harm and consequence in data breach notification policy', Dennis Gibson The University of Queensland, Australia Clive Harfield + (OAIC, 2019; Wyre et al., 2020)

Jeff Burt, 'Multi-Party Cyberattacks Lead to Big Losses: Security Researchers' (eSecurity Planet, 21 October 2021) https://www.esecurityplanet.com/threats/multi-party-cyberattacks-lead-to-big-losses/ accessed 20 August 2023

Information Technology Industry Council, *Global Policy Principles for Security Incident Reporting* (ITI, 27 September 2021) https://www.itic.org/documents/cybersecurity/ITIGlobalPolicyPrinciples-SecurityIncidentReporting.pdf accessed 8 August 2023

Information Technology Industry Council, 'ITI Recommendations for the NIS2 Trilogue Negotiations' *(ITI, February 2022)* <https://www.itic.org/documents/europe/ITINIS2TrilogueNegRecommendedTextFINAL.pdf> accessed 8 August 2023

Kamara I and van den Boom J, 'Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices' (2022) TILT Tilburg Law School

Karathanasis T, 'Member States Confronted with EU-Based Rules in the Field of Cybersecurity, The Effectiveness of Directive (EU) 2016/1148' (Phd Thesis, Université Grenoble Alpes 2022) https://theses.hal.science/tel-04077226v1/file/KARATHANASIS_2022_archivage.pdf accessed 20 August 2023

Karyda M and Mitrou L, *Data Breach Notification: Issues and Challenges for Security Management* (10th Mediterranean Conference on Information Systems MCIS, Cyprus, 2016) https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1060&context=mcis2016 accessed 8 August 2023

Kasl F, 'The US lessons for the EU personal data breach notification' (2021) 11 The Lawyer Quarterly

Kasl F, 'The US Lessons for the EU Personal Data Breach Notification: Part II – The EU Regulatory Perspective and Discussion of the Benefits Available from the US Experience' (2021) 11 The Lawyer Quarterly

Kaya M, 'Self-Disclosure or Burying the Evidence Dilemma: A Legal Review of the Data Breach Rules under the Turkish Personal Data Protection Law' (2021) 70 Annales de la Faculté de Droit d'Instanbul

Kiesow Cortez E, 'Data Breaches and GDPR' in T Holt and A Bossler (eds); *The Palgrave Handbook of International Cybercrimeand Cyberdeviance* (Palgrave Macmillan 2020)

Lucini V, 'The ever-increasing cybersecurity compliance in Europe: the NIS2 and what all businesses in the EU should be aware of' (2023) 11 Russian Law Journal

Mantelero A and others, 'The common EU approach to personal data and cybersecurity regulation' (2020) 28 International Journal of Law and Information Technology

Markopoulou D, Papakonstantinou V and de Hert P, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 1

Mc Cullagh K, Barker K and Sutter G, 'Regulating transitions in technology, law, and beyond' (2021) 35:2 International Review of Law, Computers & Technology

Michels J and Walden I, 'Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?' (2020) 25 European Law Review

Moody's Investor Service, 'Cyber – Europe: New EU cybersecurity legislation is credit positive' *(Moody's Investor Service, June 2022)* https://admin.govexec.com/media/sector_comment_-_cyber-europe_-_14jun22.pdf accessed 8 August 2023

National Cyber Security Centre, 'Coordinated Vulnerability Disclosure: The Guideline' *(NCSC, October 2018)* <https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline> accessed 8 August 2023

National Cyber Security Centre, 'Coordinated Vulnerability Disclosure: The Guideline' *(NCSC, October 2018)* <https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf> accessed 8 August 2023National Cyber Security Centre, 'Exploration of best practices for cybersecurity information sharing' (*NCSC)* https://english.ncsc.nl/research/research-results/exploration-of-best-practices-for-cybersecurity-information-sharing-map accessed 8 August 2023

Niemann F, Karniyevich N and Sickinghe F, 'NIS2 Directive EU Co-legislators reach a provisional agreement' *(Bird & Bird, June 2022)* <https://www.twobirds.com/-/media/new-website-content/pdfs/insights/2022/global/220608_nis2-directive_provisional-agreement_newsletter_final.pdf> accessed 8 August 2023

Nieuwesteeg B and Faure M, 'An analysis of the effectiveness of the EU data breach notification obligation' (2018) 34 Computer Law & Security Review

NIS Cooperation Group, 'Cybersecurity Incident Taxonomy' *(CG Publication, July 2018)* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646 accessed 8 August 2023

NIS Cooperation Group, 'Reference document on Incident Notification for Operators of Essential Services - Circumstances of Notification' *(CG Publication, February 2018)*

<https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf> accessed 8 August 2023

NIS Cooperation Group, 'Synergies in Cybersecurity Incident Reporting' *(CG Publication, April 2020)* https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group accessed 8 August 2023

Nyman M and Große C, *Are You Ready When It Counts? IT Consulting Firm's Information Security Incident Management* (5th International Conference on Information Systems Security and Privacy ICISSP, Prague, 2019) https://www.semanticscholar.org/paper/Are-You-Ready-When-It-Counts-IT-Consulting-Firm's-Nyman-Große/4ea053242400cbb2a4589787ba9dce0ab4394338 11 August 2023 26

Parajon Skinner C, 'Bank Disclosures of Cyber Exposure' (2019) 105 Iowa Law Review

Renna M, 'Data Breach Disclosure Duties' (2019) 2 European Journal of Privacy Law & Technologies (2019)

Roos A, 'Data Protection Principles under the GDPR and the POPI Act: A Comparison' (2023) 86:1 THRHR

Samardžić D, 'Records of processing activities (Art. 30 GDPR) in analogue and digital ecosystems' (2021) 14 ANALI Pravnog Fakulteta Univerziteta U Zenici

Saqib N and others, 'Mapping of the Security Requirements of GDPR and NISD' (2020) 7:24 EAI Endorsed Transactions on Security and Safety

Schmitz-Berndt S and Anheier F, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context'(2021) 7 Eur. Data Prot. L. Rev. 101

Schmitz-Berndt S and Chiara PG, 'One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive' (2022) Int. Cybersecur. Law Rev.

Schmitz-Berndt S and Cole MD, 'The Interplay between the NIS Directive and the GDPR in a Cybersecurity Threat landscape' (2019) University of Luxembourg Law Working Paper No. 2019-017

Schmitz-Berndt S and Schiffner S, 'Don't Put the Cart Before the Horse – Effective Incident Handling Under GDPR and NIS Directive' in M Friedewald, S Schiffner and S Krenn (eds), *Privacy and Identity Management* (Springer 2020)

Schmitz-Berndt S and Schiffner S, 'Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR' (2021) International Review of Law, Computers & Technology

Schmitz-Berndt S and Schiffner S, 'Responsible Vulnerability Disclosure under the NIS 2.0 Proposal' (2021) 12 JIPITEC 447

Schmitz-Berndt S, 'Cybersecurity is Gaining Momentum - NIS 2.0 is on its Way' (2021) 7 European Data Protection Law Review 580

Schmitz-Berndt S, 'Defining the reporting threshold for a cybersecurity incident under the NIS 2 Directive' (2023) Journal of Cybersecurity 1, 7-9

Schmitz-Berndt S, '*Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes'* in C Onwubiko et al (eds); *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media* (Springer 2023)

Sievers T, 'Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations' (2021) 2 Int. Cybersecur. Law Rev.

Skias D et al, 'Demonstration of alignment of the Pan-European Cybersecurity Incidents Information Sharing Platform to Cybersecurity policy, regulatory and legislative advancements' (17th International Conference on Availability, Reliability and Security ARES, New York, 2022) https://dl.acm.org/doi/pdf/10.1145/3538969.3544477

Skopik F, Settanni G and Fiedler R, 'A problem shared is a problem halved: A survey on the dimension of collective cyber defense through security information sharing' (2016) 60 Computers & Security

Verstraete M and Zarsky T, 'Optimizing Breach Notification' (2020) 2021 University of Illinois Law Review

Voigt P and dem Bussche A, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (1st edn, Springer 2017)

Wang F, 'Personal Data Breach Notification System in the European Union: Interpretation of "Without Undue Delay"' (2011) 22:6 European Business Law Review

Weulen Kranenbarg M, Holt T and van der Ham J, 'Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure' (2018) 7:16 Crime Science

Zygierewicz A, 'Implementation Appraisal: Directive on security of network and information systems (NIS Directive)' (*European Parliamentary Research Service, November 2020)*

<https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf> accessed 8 August 2023