**Legal Aspects of Vulnerability Disclosure: Navigating GDPR and NIS Directive Obligations for Data Protection and Cybersecurity**

**Ana Koiava[[1]](#footnote-1)**

**Tallinn University of Technology**

# ***Abstract***

*The disclosure of vulnerabilities in the context of data protection and cybersecurity raises numerous legal aspects that require careful navigation. This paper examines the legal implications of vulnerability disclosure within the context of data protection and cybersecurity, with a specific focus on the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS2) Directive. The research problem addressed in this study is the need to understand the legal obligations and challenges associated with vulnerability disclosure under these regulatory frameworks.*

*The research aims to explore the legal requirements, identify conflicts, and provide insights into vulnerability disclosure practices. The study employs a methodology that involves a comprehensive review and analysis of legal documents, guidelines, and scholarly literature. This approach allows for a thorough examination of the legal aspects surrounding vulnerability disclosure. The findings contribute to a better understanding of the legal landscape and provide valuable insights.*

***Keywords:*** *EU, Cybersecurity, GDPR, NIS2D, Vulnerability Disclosure*

# Introduction

In today's digital landscape, the discovery and disclosure of vulnerabilities have become critical concerns that require careful attention and adherence to legal obligations. The disclosure of vulnerabilities has been a topic of debate within the information security community for a considerable period. The urgency to address cybersecurity and software vulnerabilities stems from the increasing connectivity of devices and individuals[[2]](#footnote-2). The General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS2) Directive are two key legal frameworks that aim to safeguard data protection and cybersecurity within the European Union (EU)[[3]](#footnote-3). Navigating the obligations imposed by these regulations when disclosing vulnerabilities is of utmost importance to ensure compliance, protect personal data, and maintain a secure online environment. These efforts promote accountability, uphold the rule of law, and contribute to a safer digital environment for all while ensuring the protection of personal data[[4]](#footnote-4). This article examines the legal aspects of vulnerability disclosure and explores the challenges and considerations involved in balancing the requirements of the GDPR and the NIS2 Directive.

The primary focus of this research is the examination of the legal aspects associated with vulnerability. Thus, it is essential to establish a comprehensive understanding of the concept of vulnerability in order to address these legal considerations effectively[[5]](#footnote-5). Vulnerabilities are typically defined by three fundamental characteristics. Firstly, they involve the existence of a flaw or weakness within a system, serving as a potential entry point for attackers. Secondly, vulnerabilities possess the capacity for threats, including hackers, to exploit the identified flaw. Lastly, the exploitation of vulnerabilities can result in compromised information security, posing a significant risk to both software and hardware systems[[6]](#footnote-6). These elements collectively highlight the potential dangers that vulnerabilities pose to the overall security of digital environments.

# Challenges Regarding vulnerability disclosure

Vulnerability disclosure involves the process of identifying, reporting, and resolving weaknesses in software, hardware, or services that have the potential to be exploited[[7]](#footnote-7). The vulnerability disclosure process presents a range of significant challenges that must be effectively addressed. These challenges include navigating complex legal considerations, as individuals disclosing vulnerabilities may face potential legal threats due to the methods used and the manner of disclosure. The acquisition of vulnerabilities for national security purposes may result in intentional non-disclosure, leaving users vulnerable without a solution. User’s failure to implement patches promptly further exacerbates the risks, often due to a lack of understanding or knowledge. Moreover, variations in discoverer motivation, influenced by bug bounty programs and monetary rewards, can impact the disclosure decisions made.[[8]](#footnote-8) To overcome these challenges, it is crucial to carefully consider these factors and establish effective mechanisms that promote responsible vulnerability disclosure, prompt patch implementation, and foster collaboration among all stakeholders involved.

The process of vulnerability disclosure refers to the steps taken to handle the dissemination of software vulnerability knowledge after it has been identified by a user. Responsible vulnerability disclosure aims to minimize the negative impact of vulnerabilities by determining how and when vulnerability information should be shared with the appropriate parties through the appropriate channels[[9]](#footnote-9). The lack of consensus arises from the fact that vulnerability information has varying relevance to different stakeholders, including the software vendor, software users, and potential hackers. The way vulnerability knowledge is managed, including the sequence and timing of its announcement, can significantly impact the overall cost of the vulnerability to society[[10]](#footnote-10).

The disclosure of vulnerabilities raises significant questions due to the sensitive nature of the information involved. These questions arise from the presence of diverging and conflicting interests among stakeholders, as well as legal constraints on their actions[[11]](#footnote-11). As digital and software-dependent technologies become more integrated into everyday life, it becomes essential for the economy and society as a whole to establish appropriate procedures for vulnerability disclosure. While it is clear that vulnerability disclosure is necessary from the perspective of end-users such as businesses and home users, important questions remain unanswered. It is essential to address several critical aspects when it comes to disclosure, including identifying the responsible party, establishing the appropriate disclosure methods, and determining the right timing for making vulnerabilities public. Careful consideration and consensus among stakeholders are vital to safeguard the security of end-users[[12]](#footnote-12).

Vulnerability disclosure entails several important legal aspects that must be considered to ensure responsible and lawful practices. These aspects include adhering to legal rights and obligations, establishing responsible disclosure policies, maintaining confidentiality and non-disclosure agreements, complying with personal data protection laws, coordinating with relevant authorities, ensuring liability protection, and considering public interest implications. It is crucial for individuals and organizations engaged in vulnerability disclosure to navigate these legal aspects carefully and collaborate with researchers, software vendors, security organizations, and legal experts to ensure compliance and protect the rights and interests of all parties involved[[13]](#footnote-13).

It is worth noting that two crucial legal instruments, namely the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS2) Directive, were implemented to uphold adequate security standards for information technology (IT) and its associated data processing. While both the GDPR and the NIS2 Directive incorporate risk-based security measures, they serve distinct purposes and objectives.[[14]](#footnote-14)

The GDPR is a comprehensive data protection regulation in the European Union that establishes rules and requirements for the protection of personal data. It emphasizes the importance of data security and imposes obligations on organizations to ensure the confidentiality, integrity, and availability of personal data. Vulnerability disclosure is closely tied to data security, and organizations are expected to promptly address and disclose vulnerabilities that may impact the security of personal data[[15]](#footnote-15).

The NIS2 Directive, on the other hand, focuses on the security of network and information systems in critical sectors such as energy, transportation, banking, and healthcare. It sets out requirements for risk management, incident reporting, and cooperation between member states. Vulnerability disclosure is crucial in the context of the NIS2 Directive, as timely reporting and handling of vulnerabilities can help prevent security incidents and mitigate risks to critical infrastructure[[16]](#footnote-16).

NIS2 Directive prioritizes the availability of services, with confidentiality and integrity being secondary considerations. It is worth noting that information security incidents can often impact personal data. While the NIS2 Directive has a broader scope, covering digital data related to network and information systems and their provision and continuity, it is more limited in terms of its applicability, targeting only identified operators of essential services (OES) and digital service providers[[17]](#footnote-17). These legal instruments work together to establish a comprehensive framework for protecting data and ensuring the security of IT systems. The GDPR focuses on the rights and privacy of individuals, while the NIS2 Directive concentrates on the resilience and security of critical infrastructures[[18]](#footnote-18).

# Reporting Obligations

This article aims to analyze the reporting requirements prescribed by the NIS 2 Directive and the GDPR, with a focus on highlighting the similarities and differences between these regulatory frameworks. Both directives impose obligations on organizations to report incidents, however, they diverge in terms of their scope. The NIS 2 Directive centers on incidents concerning network and information systems that have an impact on essential services, while the GDPR primarily concerns personal data breaches. By examining these aspects in detail, this study seeks to provide a comprehensive understanding of the incident reporting processes within the purview of both frameworks.

## 3.1 Data Breach Reporting in Accordance with the GDPR

The issue of data breach reporting under the GDPR is intricately intertwined with vulnerability disclosure and cybersecurity challenges. In the event of a data breach, it is common for the breach to exploit vulnerabilities within a system, resulting in unauthorized access, data leakage, or other security-related incidents.

Under the General Data Protection Regulation (GDPR), organizations are required to report data breaches that pose a risk to individuals' rights and freedoms. This reporting obligation is outlined in Article 33 of the GDPR. Article 33 states that in the event of a data breach, data controllers must notify the supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach. The notification should include details such as the nature of the breach, the categories and an approximate number of affected individuals, the likely consequences of the breach, and the measures taken or proposed to address the breach and mitigate its effects[[19]](#footnote-19).

In addition, the provision outlined in Article 34 of the GDPR, which mandates the communication of data breaches to affected individuals, serves a crucial purpose in enhancing transparency and accountability in data protection practices. By requiring data controllers to promptly notify individuals of breaches that pose a high risk to their rights and freedoms, the GDPR aims to empower individuals and regulatory authorities with timely information to take necessary actions and mitigate potential harm. The requirement for clear and easily understandable communication ensures that individuals can comprehend the breach and comprehend the recommended steps to safeguard themselves.[[20]](#footnote-20) Nonetheless, challenges arise from subjective risk evaluation, ambiguous reporting timelines, and individuals' limited awareness. Resolving these issues requires clear guidelines to standardize risk assessment and reporting, alongside cybersecurity measures to enhance breach notifications, safeguard individual rights, and minimize harm.

Organizations must prioritize their understanding of the specific requirements outlined in Articles 33 and 34 of the GDPR. They should establish robust processes and procedures to promptly and efficiently handle data breaches. Non-compliance with these reporting obligations can lead to severe penalties and reputational harm for organizations. Hence, taking proactive steps to comply with the GDPR's data breach reporting requirements is essential to safeguard the organization's reputation, maintain regulatory compliance, and protect individuals' rights and privacy.

## 3.2 Incident Reporting Obligations under the NIS Directive

On the Other hand, NIS Directive 2 (Network and Information Systems Directive 2) is a regulatory framework introduced by the European Union to strengthen cybersecurity measures and protect critical infrastructure and digital services. A significant component of NIS2 is the establishment of a comprehensive framework for coordinated vulnerability disclosure[[21]](#footnote-21). Under NIS2, key actors are assigned specific responsibilities in handling newly discovered vulnerabilities throughout the European Union. This coordinated approach ensures that vulnerabilities are promptly and responsibly disclosed to relevant parties, minimizing the potential risks they pose[[22]](#footnote-22).

Additionally, NIS2 mandates the creation of an EU vulnerability database, managed and maintained by the EU Agency for Cybersecurity (ENISA). This database serves as a central repository for publicly known vulnerabilities in information and communication technology (ICT) products and services[[23]](#footnote-23). One of the strengths of this approach is the potential for a centralized and comprehensive database that can streamline vulnerability management efforts. Having a single repository can facilitate efficient identification, tracking, and mitigation of vulnerabilities across various ICT products and services. This can lead to faster patching and improved security measures, reducing the risk of cyber incidents and enhancing overall cybersecurity posture.[[24]](#footnote-24)

NIS2 presents a holistic structure for businesses, comprising 10 essential components that need to be acknowledged and incorporated into their cybersecurity protocols. These components span a range of domains, including incident management, safeguarding the supply chain, handling and disclosing vulnerabilities, and responsibly employing cryptography and encryption.[[25]](#footnote-25)

When it comes to incident reporting, striking the right balance between swift reporting and in-depth analysis is crucial. The new Directive adopts a multi-stage approach to incident reporting. In the event of an incident, companies have a 24-hour window from the time they become aware of it to submit an early warning to the Computer Security Incident Response Team (CSIRT) or the competent national authority. This early warning also enables companies to seek assistance, such as guidance or operational advice on implementing mitigation measures if needed[[26]](#footnote-26). Following the early warning, companies are required to provide an incident notification within 72 hours of becoming aware of the incident.[[27]](#footnote-27) Finally, affected companies must submit a final report no later than one month after becoming aware of the incident. By adopting this multi-stage approach to incident reporting, NIS2 aims to strike a balance between prompt reporting to prevent incident escalation and detailed reporting to extract valuable insights from each incident[[28]](#footnote-28). This iterative reporting process enhances incident management capabilities, strengthens cybersecurity practices, and contributes to a more resilient and secure digital environment.

Yet, the 24-hour reporting window in the multi-stage incident reporting approach poses challenges. Rushed reporting may hinder thorough incident analysis, understanding of causes, and impact. Balancing speed with accuracy is crucial. Effective implementation relies on capable authorities providing timely assistance. Insufficient resources or expertise may hinder support to organizations. Smaller organizations may struggle to meet reporting requirements promptly, considering limited resources. Addressing challenges for all organizations is important for effective incident reporting systems.

# Balancing GDPR and NIS Directive 2

The disclosure obligations in both the GDPR and the NIS2 Directive share some similarities. Both frameworks require organizations to report incidents, although the scope of reporting differs. The differing objectives of the GDPR and the NIS2 Directive can create challenges when it comes to advising on incident notification. The GDPR places a strong emphasis on safeguarding personal data and advocates for immediate notification to enable affected individuals to mitigate potential harm. In contrast, the NIS2 Directive is primarily concerned with restoring and maintaining information security, and incident disclosure under this framework may be limited to cases where public awareness is crucial for preventing or addressing ongoing incidents or when disclosure serves the public interest.

Recital 86 of the GDPR recognizes the challenge of early disclosure and acknowledges the need for prompt communication with data subjects to mitigate immediate risks. However, this justification specifically applies to continuing and ongoing data breaches and does not cover ongoing security incidents in general[[29]](#footnote-29). As a result, incidents that inadvertently compromise consumer data but lead to ongoing attacks on other critical systems may not be adequately addressed. It is important to note that while Recital 86 provides interpretative guidance, it does not establish legally binding limits on the scope of Article 34 of the GDPR, which governs incident notification. Additionally, when determining administrative fines for non-compliance with Article 34, the effectiveness of incident mitigation and an appropriate NIS response are factors considered[[30]](#footnote-30).

The GDPR does not have explicit regulations that specifically cover incident containment and recovery, or provide exceptions for delaying the notification of data subjects in cases involving law enforcement or other relevant interests. This ongoing disagreement persists due to the absence of such provisions in the GDPR framework[[31]](#footnote-31).

However, the NIS 2.0 Proposal resolves one aspect of the conflict by eliminating the possibility of facing legal consequences for non-compliance under both the GDPR and the NIS instrument[[32]](#footnote-32). Article 32(2) of the NIS 2.0 Proposal clarifies that if a Data Protection Authority (DPA) imposes an administrative fine, a National Competent Authority (NCA) cannot impose an additional administrative fine for the same infringement. It is important to note that failing to comply with notification obligations towards the regulatory authority and failing to comply with the notification obligation towards the data subject or service recipient are considered separate infringements[[33]](#footnote-33).

To explore deeply, the division of notification obligations in NIS2 may lead to a fragmented incident reporting approach. Organizations might prioritize fulfilling their duties towards the regulatory authority, potentially neglecting their obligations towards affected individuals or service recipients. This neglect has the potential to compromise the rights and interests of individuals whose personal data is impacted by the incident. Consequently, an entity that informs the DPA and NCA about a security incident involving personal data but fails to inform the data subject without undue delay to handle the incident may potentially face legal sanctions under the GDPR[[34]](#footnote-34).

# Conclusion

In conclusion, this research has highlighted the legal aspects of vulnerability disclosure in connection with data protection and cybersecurity. The conflicting objectives of the GDPR and the NIS2 Directive create a delicate balance between immediate data protection notification and the need for the delay to address cybersecurity concerns.

It is essential to acknowledge and address the inherent limitations and challenges associated with this research. The dynamic nature of legal frameworks introduces ongoing complexities as regulations and guidelines evolve over time. Furthermore, successfully navigating vulnerability disclosure requires careful management of the intricate interplay between data protection and cybersecurity considerations.

Despite these challenges, this research provides valuable insights into the legal landscape surrounding vulnerability disclosure. By thoroughly understanding the explicit requirements outlined in the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS2) Directive, organizations can enhance their incident reporting practices while ensuring diligent compliance with regulatory obligations.

To thrive in this ever-changing environment, organizations must maintain constant vigilance, continuously monitoring and adapting to changes in legal frameworks. It is of utmost importance to carefully consider and balance both data protection and cybersecurity aspects when disclosing vulnerabilities. Through these measures, organizations can effectively mitigate risks, protect individuals' data, and contribute to the creation of a safer and more secure digital ecosystem.

**BIBLIOGRAPHY/** **References**

**Primary Resources / EU Legislation**

Coordinated vulnerability disclosure practices in the EU, April 2022, European Union Agency for Network and Information Security.

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Retrieved from, <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive> 15 May 2023.

Good Practice Guide on Vulnerability Disclosure From challenges to recommendations November 2015, European Union Agency for Network and Information Security.

NIS Cooperation Group, Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>, 20 May 2023.

Technology, Policies and Legal Challenges Report of a CEPS Task Force, June 2018, Chair: Marietje Schaake Rapporteurs: Lorenzo Pupillo Afonso Ferreira Gianluca Varisco.

Vulnerability Disclosure, <https://www.enisa.europa.eu/topics/vulnerability-disclosure>, 20 May 2023.

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.

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).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

**Scholarly Articles**

Cavusoglu, H., Raghunathan, S. (2007). The efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge*. IEEE Transactions on Software Engineering*, 33(3), 171–185.

Mazur, V.; Chochia, A. (2022). Definition and Regulation as an Effective Measure to Fight Fake News in the European Union. European Studies: The Review of European Law, Economics and Politics, 9 (1), 15−40. DOI: 10.2478/eustu-2022-0001.

Federal Association for Information Technology, Telecommunications and New Media. 13 August 2020. Roadmap NIS-Review Bitkom views concerning the combined Evaluation Roadmap / Inception Impact Assessment.

Schmitz-Berndt, Sandra, Schiffner Stefan (2021), Don’t tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR, *International Review of Law, Computers, and Technology*, 35:2, 101-115.

Schmitz Sandra and Stefan Schiffner, 2021 Responsible Vulnerability Disclosure under the NIS 2.0 Proposal.

Tropp, E.-M.; Hoffmann, T.; Chochia, A. (2022). Open Data – a stepchild in e-Estonia’s Data Management Strategy? TalTech Journal of European Studies, 12 (1 ), 123−144. DOI: 10.2478/bjes-2022-0006.

1. Project Assistant, Department of Law, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia

Email: ankoia@taltech.ee [↑](#footnote-ref-1)
2. Technology, Policies and Legal Challenges Report of a CEPS Task Force, June 2018, Chair: Marietje Schaake Rapporteurs: Lorenzo Pupillo Afonso Ferreira Gianluca Varisco [↑](#footnote-ref-2)
3. Tropp, E.-M.; Hoffmann, T.; Chochia, A. (2022). Open Data – a stepchild in e-Estonia’s Data Management Strategy? TalTech Journal of European Studies, 12 (1 ), 123−144. DOI: 10.2478/bjes-2022-0006. [↑](#footnote-ref-3)
4. Technology, Policies and Legal Challenges Report of a CEPS Task Force, June 2018, Chair: Marietje Schaake Rapporteurs: Lorenzo Pupillo Afonso Ferreira Gianluca Varisco [↑](#footnote-ref-4)
5. *See also:* Mazur, V.; Chochia, A. (2022). Definition and Regulation as an Effective Measure to Fight Fake News in the European Union. European Studies: The Review of European Law, Economics and Politics, 9 (1), 15−40. DOI: 10.2478/eustu-2022-0001. [↑](#footnote-ref-5)
6. Good Practice Guide on Vulnerability Disclosure From challenges to recommendations, November 2015,European Union Agency for Network and Information Security [↑](#footnote-ref-6)
7. Vulnerability Disclosure, <https://www.enisa.europa.eu/topics/vulnerability-disclosure>, 20 May 2023 [↑](#footnote-ref-7)
8. Good Practice Guide on Vulnerability Disclosure From challenges to recommendations November 2015, European Union Agency for Network and Information Security [↑](#footnote-ref-8)
9. Cavusoglu, H., Raghunathan, S. (2007). The efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge*. IEEE Transactions on Software Engineering*, 33(3), 171–185. [↑](#footnote-ref-9)
10. *Ibid* [↑](#footnote-ref-10)
11. Technology, Policies and Legal Challenges Report of a CEPS Task Force, June 2018, Chair: Marietje Schaake Rapporteurs: Lorenzo Pupillo Afonso Ferreira Gianluca Varisco [↑](#footnote-ref-11)
12. *Ibid.* [↑](#footnote-ref-12)
13. *Ibid.* [↑](#footnote-ref-13)
14. Sandra Schmitz-Berndt, Stefan Schiffner (2021) Don’t tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR, *International Review of Law, Computers and Technology*, 35:2, 101-115. [↑](#footnote-ref-14)
15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [↑](#footnote-ref-15)
16. 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. [↑](#footnote-ref-16)
17. 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. [↑](#footnote-ref-17)
18. *Sandra Schmitz-Berndt, Stefan Schiffner. Op.cit.,*  [↑](#footnote-ref-18)
19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 33. [↑](#footnote-ref-19)
20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 34. [↑](#footnote-ref-20)
21. NIS Cooperation Group, Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>, 20 May 2023 [↑](#footnote-ref-21)
22. NIS Cooperation Group, Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>, 20 May 2023 [↑](#footnote-ref-22)
23. Coordinated vulnerability disclosure practices in the EU, April 2022, European Union Agency for Network and Information Security [↑](#footnote-ref-23)
24. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Retrieved from, <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive> 15 May 2023 [↑](#footnote-ref-24)
25. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Retrieved from, <https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive> 15 May 2023 [↑](#footnote-ref-25)
26. 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), Article 23, 4(a) [↑](#footnote-ref-26)
27. 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), Article 23, 4(b) [↑](#footnote-ref-27)
28. 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), Article 23, 4 (c, d) [↑](#footnote-ref-28)
29. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 86. [↑](#footnote-ref-29)
30. Sandra Schmitz and Stefan Schiffner , 2021 Responsible Vulnerability Disclosure under the NIS 2.0 Proposal [↑](#footnote-ref-30)
31. Position Paper – Roadmap NIS-Review Bitkom views concerning the combined Evaluation Roadmap / Inception Impact Assessment, 13 of August 2020 [↑](#footnote-ref-31)
32. Sandra Schmitz and Stefan Schiffner , 2021 Responsible Vulnerability Disclosure under the NIS 2.0 Proposal [↑](#footnote-ref-32)
33. 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), Article 32(2) [↑](#footnote-ref-33)
34. *Ibid.* [↑](#footnote-ref-34)