MARIANA MACHADO AIRES
8876

THE GDPR AND PERSONAL DATA BREACHES: A FOCUS ON THE EFFECTIVENESS OF ARTICLE 33 AND HOW IT CAN BE BETTER ENFORCED

Dissertation to obtain a Master's Degree in Law, in the specialty of Business Law and Technology

Supervisor:
Professor Dr. Vera Lúcia Raposo, Professor of the NOVA School of Law

April 2025

MARIANA MACHADO AIRES
8876

THE GDPR AND PERSONAL DATA BREACHES: A FOCUS ON THE EFFECTIVENESS OF ARTICLE 33 AND HOW IT CAN BE BETTER ENFORCED

Dissertation to obtain a Master's Degree in Law, in the specialty of Business Law and Technology

Supervisor:
Professor Dr. Vera Lúcia Raposo, Professor of the NOVA School of Law

April 2025

ANTI-PLAGIARISM STATEMENT

I hereby declare that the work I present, is my own work and that all my citations are correctly acknowledged.

I am aware that the use of unacknowledged extraneous materials and sources, constitutes a serious ethical and disciplinary offence.

Lisbon, April 2025

Mariana Machado Aires (student no. 8876)

"*Privacy isn't something to hide.*
Privacy is about something to protect."

Edward Snowden

DEDICATION AND AKNOWLEDGEMENTS

Firstly, I would like to express my gratitude to my supervisor, Professor Vera Lúcia Raposo. Thank you for your help, comprehension and guidance throughout this journey. Your passion for topics like Privacy and Security and the GDPR are an inspiration to every Law and Tech geek out there!

To my parents, who gave me all the resources to be where I am today and who motivate me every day to be a better version of myself. You are the foundation of my life – thank you for your sacrifices and unconditional love and support.

To my sister, my best friend in the whole world. I know I do not say this enough, but your determination and dedication, both personally and professionally, inspire me every day.

To my grandmother, thank you for all the candles you lit during my academic path. I would not have succeeded without them.

To my friends from the Faculty of Law of the University of Lisbon, Madalena F., Sofia N., Sara P., Sofia G., and Beatriz M., who have accompanied me since the beginning of my academic journey. This one is dedicated to you, because you have been with me through the ups and downs and always gave me a helping hand when I needed the most. Only you truly understand what it means to complete another step! Thank you for being the best of friends and for putting with my countless questions.

To my "sister from another mister", Benedita C., I am grateful that our lives crossed paths at NOVA School of Law. Thank you for your friendship and for understanding me like no one else.

To my mentors, Ana S. and Ana M. Thank you for introducing me to data protection, it was you that made me want to pursue this field. Thank you for the opportunity to work and learn from you and for always pushing and inspiring me to do and be better at what I do. I am forever thankful for your guidance, patience and encouragement.

And, finally, to Pedro E. Thank you for being my 'partner in privacy' and for being as much of a geek as I am when it comes to privacy and cybersecurity. Thank you for your ideas and expertise on information security. They were a great contribution to the writing of this dissertation.

QUOTING AND OTHER CONVENTIONS

For the present dissertation, we opted to cite using the American Psychology Association's style (APA, 7th edition).

LIST OF ABBREVIATIONS

AP – Autoriteit Persoonsgegevens (Dutch Data Protection Authority)

EDPB – European Data Protection Board

DPA – Data protection authority

DPC – Data Protection Commission (Irish Data Protection Commission)

DPLED – Data Protection Law Enforcement Directive

DPO – Data protection officer

GDPR – General Data Protection Regulation

ISMS – Information security management system

OECD – Organization for Economic Co-operation and Development

NGO – Non-governmental organization

SA – Supervisory authority

UODO – Urząd Ochrony Danych Osobowych (Polish Data Protection Authority)

WP29 – Article 29 Working Party

DECLARATION

O corpo da presente dissertação, incluindo espaços e notas, ocupa um total de 134,926 caracteres.

The body of the present dissertation, including spaces and footnotes, occupies a total of 134,926 characters.

ABSTRACT

The topic we propose to investigate throughout our dissertation is personal data breaches, the effectiveness of Article 33 of the GDPR, and approaches for its improved enforcement.

The GDPR has established itself as a global standard for data protection, mandating that controllers must notify the competent SA's of personal data breaches within 72 hours after becoming aware of them. However, many of these breaches remain unreported due to inconsistent enforcement, administrative burdens, and concerns over reputational damage.

Key challenges include detecting and assessing personal data breaches within the required timeframe, which may be insufficient given the complexity of modern cyber threats, and differentiating between security incidents and personal data breaches. The risk of severe sanctions may also lead to under-deterrence, where organizations avoid reporting personal data breaches to escape sanctions, or over-deterrence, where they report excessively to mitigate potential consequences.

A more flexible approach, such as the NIS 2 Directive's two-tiered notification model, could enhance notification efficiency. Organizations, in order to strengthen compliance and enforcement, should also adopt comprehensive data protection policies, standardized security mechanisms, and efficient incident response plans.

Enhancing regulatory oversight and refining notification criteria can lead to a more effective enforcement of Article 33 of the GDPR, ultimately fortifying the EU data protection framework and ensuring stronger safeguards for data subjects.

Keywords: data protection, privacy law, GDPR, personal data breaches, security incidents, personal data breach notification, regulatory compliance, cyber threats, data protection authorities, incident response, risk assessment

RESUMO

O tema que nos propomos a investigar ao longo da nossa dissertação são as violações de dados pessoais, a eficácia do Artigo 33.º do RGPD e as estratégias para melhorar o seu cumprimento.

O RGPD estabeleceu-se como uma referência global para a proteção de dados, exigindo que os responsáveis pelo tratamento comuniquem as violações de dados pessoais no prazo de 72 horas após terem conhecimento das mesmas. No entanto, muitas destas violações continuam a não ser comunicadas devido a um cumprimento inconsistente, sanções e apreensão face aos danos reputacionais.

Os principais desafios incluem a deteção e avaliação das violações de dados pessoais dentro do prazo exigido, que pode ser insuficiente dada a complexidade das ciber ameaças modernas, e a diferenciação entre incidentes de segurança e violações de dados pessoais. O risco de sanções severas pode também levar a uma tendência em que as organizações evitam comunicar violações de dados pessoais para escapar às sanções ou, pelo contrário, optem por notificar em excesso para minimizar potenciais consequências.

Uma abordagem mais flexível, como o modelo de notificação em dois passos da Diretiva SRI 2, poderia aumentar a eficiência da notificação. Para reforçar a conformidade e a implementação, as organizações devem também adotar políticas abrangentes de proteção de dados, mecanismos de segurança normatizados e planos eficientes de resposta a incidentes.

O reforço da supervisão regulamentar e o aperfeiçoamento dos critérios de notificação podem conduzir a uma aplicação mais eficaz do Artigo 33.º do RGPD, reforçando, em última instância, o quadro de proteção de dados da UE e garantindo uma maior proteção aos titulares dos dados.

Palavras-chave: proteção de dados, direito da privacidade, RGPD, violações de dados pessoais, incidentes de segurança, notificação de violação de dados pessoais, conformidade normativa, ciber ameaças, autoridades de proteção de dados, resposta a incidentes, avaliação de riscos

TABLE OF CONTENTS

1. Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) (hereinafter 'GDPR'), was adopted by the European Parliament and the Council of the European Union in April 2016 and came into force in May 2018. Nevertheless, this Regulation was not the first one to regulate data and privacy.

Despite several mentions in the past, society first had contact with privacy with the Universal Declaration of Human Rights, ratified in November 1948 by United Nations' General Assembly. The right to privacy is not recognized in the Declaration, however there is a mention to it on Article 12: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*".[1]

Only two years after that, in 1950, the European Convention on Human Rights was signed and established the "*right to respect for private and family life*" on its Article 8: "*Everyone has the right to respect for his private and family life, his home and his correspondence*".[2]

However, privacy and data have not always been 'hand in hand'. As years went by, the Internet was invented and technology slowly became a part of everyone's day-to-day lives. That is why the need to regulate data and privacy became a topic.

In 1980, the Organization for Economic Co-operation and Development (hereinafter 'OECD') took the first step and adopted the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The organization recognized that while wider and inventive employs of personal data have better economic and social advantages, they also pose risks to privacy. So, the Member countries must share a common interest in promoting and defending the cores principles of privacy, individual liberties and the free flow of information across the globe.[3]

It is one of the first times in history that we are presented with concepts, such as 'personal data' and 'data controller', principles, as the principle of accountability, and data

[1] Universal Declaration of Human Rights, proclaimed on December 10, 1948, by the United Nations General Assembly.
[2] European Convention of Human Rights, signed on November 4, 1950, and effective as of September 3, 1953, by the Council of Europe.
[3] Recommendation of the Council concerning Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data, adopted on September 23, 1980, by the Organization for Economic Co-operation and Development.

subject's rights, like the ability to ask a data controller for an assurance of whether or not it has data about them.[4]

However, these Guidelines were non-binding, so most countries did nothing to implement them. But this changed in 1981, when the Council of Europe signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the first ever legally binding international instrument to regulate data and privacy.[5]

Pursuant to Article 1 of the Convention, "*the purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*."[6]

Accordingly, and in line with Article 4(1) of the Convention, all Council of Europe members, including non-members that have joined the treaty,[7] must implement the necessary measures in their national laws to uphold the fundamental principles of data protection.[8] So, it is safe to say that privacy rights are intrinsically connected with technology. However, it was only in the 1990s that the EU recognized that was time to develop a new framework that established minimum data privacy and security standards. As a result of this, the European Parliament and the Council of the European Union enacted the Directive 95/46/EC, also known as the Data Protection Directive, in October 1995.[9]

This Directive, just like the Convention for the Protection of Individuals with regard to Automatic Processing of Personal data, established in its Article 1(1) that "M*ember States shall protect the fundamental rights and freedoms of natural persons, and in particular to their right to privacy with respect to the processing of personal data*".[10]

As mentioned previously, the OECD paved the way when adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data and the principles

[4] Recommendation of the Council concerning Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data, adopted on September 23, 1980, by the Organization for Economic Co-operation and Development.
[5] This Convention has now more than 40 years and a modernized version, known as the Convention 108+.
[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed on January 28, 1981, and entered into force on October 1, 1985, by the Council of Europe.
[7] Countries like Argentina, Cabo Verde, Mexico, Senegal and Tunisia, including others, joined the treaty.
[8] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed on January 28, 1981, and entered into force on October 1, 1985, by the Council of Europe.
[9] Wolford, B. (2023). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/
[10] Directive 95/46/EC (Data Protection Directive) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

established in Part Two of these were later incorporated in Article 6 of the Data Protection Directive.

With the new century, technology evolved very swiftly and took over everything. Given the fact that we now live in an increasingly global and digital world, it was imperative for the EU to adopt a new framework that took this into account, as well as the risks of the digital age. Thus, we were presented with the GDPR – the Regulation that superseded the Data Protection Directive.

According to its Article 1(1), the Regulation "*lays down the rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*",[11] and it does so by establishing the fundamental rights of individuals in the digital era, the responsibilities of data controllers and processors, mechanisms for ensuring compliance and sanctions in the event of violations.[12]

The GDPR is considered to be the most comprehensive and strongest data protection law in the world, not only due to its broad territorial scope, but also because it establishes the protection of personal data as a fundamental right.[13] Consolidated in Article 8 of the EU Charter of Fundamental Rights, the GDPR affirms that data subjects have the right to the protection of their personal data, along with clear rights to access, rectify, and erase that data. In contrast, the Data Protection Directive, while an important step in harmonizing data protection across the EU, did not explicitly establish many of these individual rights in a direct or enforceable manner. Moreover, its territorial scope was limited – under Article 4, it primarily applied to controllers established within the EU or using EU-based data processing equipment. The GDPR, by contrast, significantly expands this scope through its Article 3, applying to any organization that processes the personal data of individuals in the EU, regardless of where the organization is located.[14]

More importantly, the GDPR marks a shift from a fragmented approach to a directly applicable regulation that provides a coherent and enforceable framework for data subjects

[11] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[12] European Council of the European Union. Available at: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/
[13] Pereira da Silva, J. (2024). *Direitos Fundamentais para o Universo Digital*. Fundação Francisco Manuel dos Santos.
[14] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

rights. These rights reflect a broader commitment to individual autonomy, dignity, and control in the digital age.[15]

Many consider data to be the new gold of the digital age, especially personal data. That is why the world has witnessed an enormous increase in cyber threats, which are becoming more frequent, complex and sophisticated over time.

The European Data Protection Board (hereinafter 'EDPB') has been publishing annual reports[16] since the GDPR came into force in 2018. Despite most countries making available the number of complaints and fines in this annual report, these cover all kinds of violations of the provisions of the GDPR, so it is not possible to quantify the number of personal data breaches. Even if it were possible to reach a figure, we would never have an exact and correct number since most organizations still do not report all personal data breaches for fear of severe sanctions and reputational damage, choosing to handle all breaches of security internally.[17]

Thus, this dissertation proposes to study personal data breaches and their implications under the GDPR, mainly focusing on the effectiveness of the data breach notification obligation, established in Article 33 of the aforesaid Regulation, by exploring the cases of personal data breaches, the process behind the notification and how it can be better enforced by organizations.

It will be organized as follow: Chapter 2 examines personal data breaches and their implications under the GDPR. It provides an overview of personal data and personal data breaches, presents examples, analyzes their consequences, and explores three recent cases. Chapter 3 focuses on Article 33 of the GDPR, detailing the process of notifying a personal data breach, the communication to data subjects, legal remedies and sanctions for non-compliance, and an assessment of its overall effectiveness. Finally, Chapter 4 proposes strategies on how companies and organizations can enhance compliance with Article 33 of the GDPR.

[15] Pereira da Silva, J. (2024). *Direitos Fundamentais para o Universo Digital*. Fundação Francisco Manuel dos Santos.
[16] The last report is from 2023.
[17] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026. Page 1238.

2. Personal data breaches and their implications under the GDPR

2.1. The GDPR and personal data

Before we start exploring personal data breaches, it is relevant to understand the concept of 'personal data'. As previously mentioned, the GPDR lays down the rules on the processing by a natural or legal person of personal data regarding individuals in the EU.[18]

So, it is safe to consider the term 'personal data' as the core of the GPDR, since it is the criterion for determining the application of the Regulation. In other words, the latter only applies if data processing in the EU involves personal data.

In light of this, it is important to ask the following question: what is considered personal data under the GDPR?

According to Article 4(1) of the Regulation, "'*personal' data means any information relating to and identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person*".[19]

There are personal data that, due to their nature, are particularly sensitive. Therefore, that data require increased protection, since the context of their processing may create significant risks for the rights and freedoms of the data subject.

And what can be considered 'sensitive data'? According to Article 9(1) of the GDPR, there are special categories of personal data. These categories include personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data and biometric data, with the purpose of uniquely identifying a natural person; health-related data; and data related to an individual's sex life or sexual orientation.[20]

[18] European Commission. Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

[19] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

[20] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

These special categories of personal data, alongside with personal data about criminal convictions and offenses, must be handled with increased caution.[21]

For the processing of personal data to be lawful, (at least) one of the six legal grounds from Article 6(1) of GDPR must apply. But due to the sensitive nature of the special categories of personal data mentioned in the previous paragraph, their processing shall be prohibited, according to Article 9(1) of the GDPR. However, paragraph 2 of the same article lists some exceptions that allow these special categories of data to be processed.

2.2. Personal data breaches

The GDPR, together with the Data Protection Law Enforcement Directive (hereinafter 'DPLED'), were the first regulatory frameworks to define what a 'personal data breach' is. Nevertheless, it was not the first one to mention the term 'breach of security'.

The Directive 2002/58/EC (hereinafter 'ePrivacy Directive'), mentions on its Article 4(2) that "*in a case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk (…)*".[22]

The ePrivacy Directive was drafted to meet the needs of new emerging digital technologies, focusing on electronic communication services. This Directive was meant to complement the Data Protection Directive, applying to all matters that the latter did not specifically cover.

Despite the fact that the Data Protection Directive was repealed by the GDPR in 2018, the ePrivacy Directive is still in force to this day, as it deals with critical issues, such as confidentiality of communications, treatment of traffic data, cookies, unsolicited communications and more.

The GDPR and the ePrivacy Directive are both cornerstones of EU data protection legislation, and despite serving different purposes, they complement each other. The GPDR introduced innovations and advancements that significantly shaped the data privacy landscape, which has also impacted the ePrivacy Directive framework, such as a broad scope of application, data processing principles and data breach notifications.

[21] Bhaimia, S. (2018). The General Data Protection Regulation: the Next Generation of EU Data Protection. *Legal Information Management*, 18(1), 21-28. https://doi.org/10.1017/s1472669618000051. Page 24.
[22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Focusing now on the GDPR, and as it was previously mentioned, this Regulation was the first to outline the concept of 'personal data breaches'. According to its Article 4(12), a personal data breach can be considered as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*".[23]

The DPLED lays down the exact same concept in Article 3(11). Two years later, the Data Protection Regulation for EU Institutions also established the very same in its Article 3(16). In view of this, we can conclude that the term only appeared with the introduction of EU data protection laws.

Now moving on to a more detailed dissection of personal data breaches. According to the Article 29 Working Party (hereinafter 'WP29'), there are three information security principles that can be used to categorize the different types of personal data breaches: (i) confidentiality breach, "*where there is an authorized or accidental disclosure of, or access to, personal data*";[24] (ii) integrity breach, "*where there is an authorized or accidental alteration of personal data*";[25] and (iii) availability breach, "*where there is an accidental or unauthorized loss of access to, or destruction of, personal data*".[26]

It is important to highlight that a breach can involve confidentiality, integrity and availability of personal data simultaneously, but also any combination of the three principles.[27]

So, it is safe to say that a breach is a form of security incident. We can perceive this term through three different approaches. The first one is lack of security, which may result from a company or organization's reluctance to acknowledge its vulnerability to data breaches or from viewing security measures as too expensive to implement.[28]

A practical example to help demonstrate this can be the case of a small e-commerce company that collects customer payment information, but does not invest in proper cybersecurity measures, like encryption or regular security audits. The company's leadership

[23] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[24] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 8.
[25] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 8.
[26] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 8.
[27] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 8.
[28] Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33 41. https://doi.org/10.20448/2001.81.33.41. Page 34.

believes that implementing these measures is too costly and assumes that their business is too small to be targeted by hackers. As a result, a cyber attacker exploits a vulnerability in the company's website, gaining access to customer credit card details. This leads to financial losses for customers, reputational damage and potential legal consequences for the company, since it failed to protect the customers' personal data.

The second one is elimination of security, which can occur because of negligence in strengthening security protocols, intentional actions by insiders or outsiders to disable safeguards, accidental loss of access rights or equipment, or deliberate interference to expose vulnerabilities.[29]

An example of this could be a financial company that provides employees with encrypted USB drives to store sensitive client data securely. However, due to budget cuts, management decides to discontinue this measure, believing it to be an unnecessary expense. At the same time, an employee accidentally misconfigures access permissions, allowing unauthorized users to view confidential files. Later, a contractor working with the company, who has access to the now-unprotected files, deliberately copies and sells client information to a third party. This example highlights how security can be eliminated due to cost-cutting decisions, accidental misconfigurations, and intentional insider threats, all of which contribute to a major data compromise.

Lastly, the third one is breach of security, which can also be deliberate, like involving malicious actions, such as malware and ransomware attacks or social engineering. Alternatively, breaches can happen accidentally through errors, such as unintentional publication of personal data, misconfigured systems, weak encryption, lost devices, or misuse of access privileges.[30]

For this approach, we need to provide two examples – one that covers the intentional angle and another that covers the unintentional angle. The first example could be of an employee that falls victim to a phishing email, unknowingly granting cyber attackers access to the company's network. These attackers then deploy a ransomware, encrypting critical files and demanding payment for their release. The other example could a company that stores client data on a cloud server, but accidentally misconfigures its security settings, making the data

[29] Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33 41. https://doi.org/10.20448/2001.81.33.41. Page 34.

[30] Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33 41. https://doi.org/10.20448/2001.81.33.41. Page 34.

publicly available. A cybercriminal discovers this vulnerability and steals personal information, leading to identify theft and financial fraud. These examples illustrate how breaches of security can occur both accidentally, through misconfigurations, and deliberately, through cyberattacks, like ransomware.

A personal data breach may either be a consequence of non-compliance with the GDPR or an event the complicates the controller's ability to ensure compliance with GDPR principles, particularly with Article 5(1)(f). This provision mandates that personal data must be processed in a way that guarantees adequate security, including safeguarding against unauthorized or unlawful processing, as well as against accidental loss, destruction or damage.[31] A breach can occur when the necessary security measures are not in place, or it may arise despite the controller's compliance efforts, but in either case, it highlights a failure in maintaining the required security standards.

Nowadays, there is a great amount of discussion about security incidents and personal data breaches. But what is the main difference between these two concepts? We can agree that all personal data breaches are security incidents. However, not all security incidents are personal data breaches. Why is that? Because not every security incident involves personal data.[32] Hence the GPDR is only applicable when a breach of security compromises personal data.

2.3. Examples of personal data breaches

Personal data breaches are not only serious security incidents in themselves, but they can also be indicative of deeper vulnerabilities, often stemming from outdated or inadequate data security. These incidents may also highlight underlying weaknesses that need to be addressed. So, in general, preventing personal data breaches in advance is always preferable to responding after they happened, as many of their consequences are irreversible, as described in the next subchapter. Before a controller can completely assess the risks associated with a personal data breach – especially one caused by an external attack – it is crucial to first identify the leading cause.[33] And the leading cause is almost always related to the most common types

[31] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[32] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 8.
[33] European Data Protection Board. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification.* Version 2.0. Adopted 14 December 2021. Page 6.

of security incidents. The EDPB adopted, in December 2021, a guideline[34] where it provides practical examples (all fictitious, but realistic scenarios) of personal data breaches.

The EDPB starts by analyzing one of the most frequent causes leading to personal data breaches – ransomware attacks. These consists of a malicious code that encrypts data and, in exchange for the decryption key, the cyber attacker demands a ransom.[35] Considering the three information security principles mentioned above, this type of security incident can be considered as a breach of availability, but there can also be a breach of confidentiality[36].

To help understand these kinds of incidents, let's imagine the following scenario: the computer systems, including its back-ups, of a non-governmental organization (hereinafter NGO) were encrypted due to a ransomware attack. In order to decrypted them, the cyber attackers demanded a ransom in Bitcoin. This constitutes a breach of availability, as the NGO cannot access their data. However, if the attackers stole data (that included names and family details from impoverished children, for example), from the NGO's systems before encrypting it and threaten to release it in the dark web if the ransom is not paid, this constitutes a breach of confidentiality. Both scenarios must be notified to the competent SA, but only in the latter should the data subjects be notified, as it poses a risk to their rights and freedoms of the impoverish children and their families.

Another example is data exfiltration attacks. These type of attacks targets vulnerabilities in services offered by the data controller to third parties via the Internet, such as injection attacks or website compromising, in order to copy, exfiltrate (i.e. stealing) or misuse personal data for malicious purposes.[37] As a result of this, they are primarily breaches of confidentiality, yet, in some cases, may also involve breaches of data integrity[38].

An example of exfiltration attacks could be the following scenario: an online grocery store was attacked and the cyber attackers placed malicious code on its website. This example covers the three types of personal data breaches discussed above. If, through this malicious code, the attackers stole credit and debit card information, it would constitute a breach of confidentiality. If the attackers had deleted the database containing all users of the online grocery store, this would constitute a breach of availability. In addition, if the cyber attackers maliciously corrupted the database, this would be considered a breach of integrity. This

[34] European Data Protection Board. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification.* Version 2.0. Adopted 14 December 2021.
[35] NIST. Small Business Cyber Corner. Ransomware. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware
[36] E.g., if the ransomware involves exfiltrating (i.e., stealing) data before encrypting it.
[37] IBM. *What is Data Exfiltration?* https://www.ibm.com/think/topics/data-exfiltration
[38] E.g., if the attacker not only exfiltrates the personal data, but also corrupts or deletes it in some way.

scenario should be notified to the competent SA and also to the concerned data subjects, as their financial information was stolen, which could result in financial losses.

Cyber attackers also use social engineering[39] to gain access to personal data. These types of attacks are different from those previously mentioned, since they target human psychology, by manipulating or deceiving the data subjects into divulging their personal data.[40] Thus, it is considered a breach of confidentiality.

For example, an attacker impersonates a bank employee, even spoofing an internal telephone number of the bank, and tricks an actual employee of the bank into giving the attacker access to several data subject's financial information, such as credit card and account information. This case must also be notified to competent SA and to the data subjects, which could lead to reputational damages for the bank and financial losses for the data subjects.

Although the majority of the cases are related to security incidents from an external source, it is also important to note that there are cases of personal data breaches due to human error,[41] and these types of breaches can occur either intentionally or unintentionally, which can be very challenging for controllers to identify vulnerabilities, and are typically breaches of confidentiality. An intentional breach can occur when a malicious insider within a company deliberately accesses clients' data in order to sell it on the black market. And an unintentional breach can occur when an employee accidentally sends an email containing strategic and confidential information to the wrong recipient.[42] Both incidents are breaches of confidentiality. The first case must be notified to the competent SA, as well as to the data subjects; however, in the latter, there may be no need to notify the incident if no personal data was shared.

Related to human error, there is the loss or theft of portable devices, such as documents or devices, like laptops or cellphones.[43] These cases are often considered as breaches of confidentiality. But if the devices were not backed up, they can also be considered as a breach

[39] The most common types of social engineering attacks are phishing, vishing or baiting.
[40] Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9, 11895-11910. https://doi.org/10.1109/access.2021.3051633. Page 11895.
[41] Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522.
[42] These cases are known as mis postal.
[43] Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522. Page 5.

of availability. And if there is a theft of confidential documents, it can also be considered as a breach of integrity or availability, as they can be modified or deleted.

It is important to keep in mind that security incidents and personal data breaches are becoming more frequent and complex than ever, so the list provided by the EDPB is non-exhaustive, as there are many more examples. The examples given are purely fictional, in order to illustrate the types of security incidents mentioned.

2.4. Consequences of personal data breaches

Before we start to analyze the process of notifying personal data breaches and the effectiveness of Article 33 of the GDPR in the next chapter, it is relevant to understand the consequences of a personal data breach, since the number of these incidents are increasing exponentially every day.

A personal data breach can have a number of substantial negative effects on data subjects, that may result in physical, material or non-material damage. The GDPR provides some examples of what these damages can represent for data subjects, like the "*loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned*".[44]

Another consequence not explicitly mentioned in Recital 85 of the GDPR, yet having a significant impact on data subjects, is personal distress. When individuals' personal data is mishandled, it can lead to emotional and psychological harm. The anxiety and fear of identity theft or loss of control over one's personal information can cause significant distress.[45]

Personal data breaches pose significant legal, financial and reputational risks as well for companies and organizations that manage personal data. Looking at the reputational risk, and when a personal data breach occurs, companies and organizations often face public suspicion and criticism, as employees, customers, vendors, partners and others may view them as negligent in protecting the data entrusted to them.[46] This is why many organizations still

[44] See Recital 85 of the GDPR.
[45] Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, 135, 559-571. https://doi.org/10.1016/j.jbusres.2021.06.054
[46] Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33 41. https://doi.org/10.20448/2001.81.33.41. Page 39.

decide not to notify the competent supervisory authority (hereinafter 'SA') when they suffer a personal data breach, resolving the issue internally instead.

The financial risks are particularly high for sectors that handle personal data, as well as the special categories of personal data mentioned on Article 9(1) of the GDPR, such as healthcare, insurers, and financial services, that store or process personal data like medical records, identification numbers and credit or debit card details.[47] These industries are considered critical and prime targets for cyber criminals, as stolen data can be exploited for fraud, identity theft and other criminal activities, since data is considered to be the new gold of the digital age and holds considerable value on the black market. According to IBM, the average global cost of a data breach is 4.88 million USD, which represents a 10% increase over 2023 and the highest total ever.[48]

In light of the rapid and profound advancement of technology and the growing digital and global economy, the GDPR requires controllers to implement suitable technical safeguards and organizational measures to promptly identify if a personal data breach has occurred. This enables them to swiftly notify the relevant SA and affected individuals. The nature, severity and impact, such as the potential consequences and outcomes, of the personal data breach on data subjects must also be considered. Consequently, controllers are obligated to maintain timely awareness of any breaches to ensure they can respond appropriately.[49] However, it is essential to recognize that each personal data breach is unique. While some may be quickly and clearly identified, others may take longer to detect. Therefore, assessing the nature and seriousness of each personal data breach is crucial, as a controller's ability to become aware of a personal data breach will depend on the specific circumstances.[50] Hence the GDPR obligation to have a breach management response plan and to notify personal data breaches, that will be explored in the next chapter.

Personal data breaches are imminent and the question is not whether they will happen, but when.

[47] Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33 41. https://doi.org/10.20448/2001.81.33.41. Page 39.
[48] IBM. *Cost of a Data Breach Report 2024*.
[49] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 11.
[50] See Recital 87 of the GDPR.

2.5. What can we learn from recent cases of personal data breaches?

As previously mentioned, the number of personal data breaches are skyrocketing each year, exposing the personal data of millions of people online, despite the fact that the GDPR came into force in 2018.

Ireland, often referred to as the 'European Silicon Valley', is home to many major tech companies, such as X (formerly known as Twitter), Google, Meta Platforms (which owns Facebook, Instagram and WhatsApp), Amazon and Dropbox, for example.

Consequently, the Irish Data Protection Commission (formally known as Data Protection Commission and hereinafter referred to as 'DPC') is widely recognized for enforcing some of the largest administrative fines,[51] as these big tech companies are known for not complying with the GDPR and are frequently involved in personal data breaches.

Apart from the DPC, several other data protection authorities (hereinafter DPA or DPA's) have enforced administrative fines, based on several violations of the GDPR. However, and by taking a quick look at the GDPR Enforcement Tracker website,[52] we can conclude that few DPA's have fined organizations for late date notification of personal data breaches.[53] Most of these fines do exceed 70.000 EUR and were mostly enforced by the Polish Data Protection Authority (hereinafter 'UODO'[54]). Nevertheless, there are cases where higher fines have been imposed on big tech companies – such as the DPC decision against Twitter International Company (hereinafter 'Twitter') and the Dutch Data Protection Authority (hereinafter 'AP'[55]) against Booking.com.

So, what could this mean? That the companies are abiding by the obligation established by Article 33(1) of the GDPR? Or that organizations are not reporting these incidents to the competent DPA's, choosing to handle them internally, in fear of reputational damage and high administrative fines? Given that security incidents involving personal data are getting more and more frequent these days, it seems that the second scenario is the most accurate.

In light of this, let's take a look at several incidents involving the violation of Article 33(1) of the GDPR in order to explore its effectiveness in the following chapter.

[51] According to the Data Protection Commission Annual Report from 2023, the DPC issued 19 finalized decisions, imposing administrative fines that amount to a total of 1.55 billion EUR. Meta Platforms is DPC's most sanctioned company – in the last three years, it was fined seven times by aforementioned SA, for a combined total of more than 2 billion EUR.
[52] https://www.enforcementtracker.com/
[53] In a quick search in the website, from a total of 2.560 entries, only 43 are related to insufficient fulfillment of data breach notification obligations. And not all of them are for violation of Article 33(1) of the GDPR.
[54] Abbreviation for Urząd Ochrony Danych Osobowych.
[55] Abbreviation for Autoriteit Persoonsgegevens.

2.5.1. DPC v. Twitter

The Twitter International Company was fined by the DPC in 450.000 EUR, on 9 December 2020, for violating Articles 33(1) and 33(5) of the GDPR.

The incident was caused by a bug[56] in Twitter's design. According to the decision made by DPC, "*a user of Twitter can decide if their tweets will be "protected" or "unprotected". In the former cases, only a specific set of persons (followers) can read the user's protected tweets. The bug that resulted in this data breach meant that, if a user operating an Android device changed the email address associated with the Twitter account, their tweets became unprotected and consequently were accessible to the wider public without the user's knowledge*".[57]

According to Twitter, and as far as they could identify, the incident impacted nearly 90.000 users between 5 September 2017 and 11 January 2019. However, the company acknowledged that the bug originated on 4 November 2014, suggesting that additional users may have been affected.

Twitter did not notify the DPC until 8 January 2019, even though it had received a report about the bug on 26 December 2018. Twitter stated that "*severity of the issue – and that it was reportable – was not appreciated until 3 January 2019 at which point Twitter's incident response process was put into action*"[58] as the reason for notifying DPC within the 72-hour period established by Article 33(1) of the GDPR.

The DPC launched the inquiry on 22 January 2019. Following this, the DPC requested for more information relating to the timeline of the incident that led to the breach and to the timeline of the notification to the DPA on several different occasions. This request is necessary to allow the DPC to verify compliance with all elements of Article 33 of the GDPR.

After Twitter's submissions, the DPC decided that Twitter did not comply with its obligations under Article 33, specifically with paragraphs 1 and 5.

With regards to paragraph 1, DPC emphasized that a controller must have measures in place to ensure timely awareness of breaches, including effective agreements with processors to facilitate prompt reporting. The controller's notification obligations begins not only when it

[56] A bug is an error, flaw or defect in a software program, causing it to produce incorrect or unintended results or crash.
[57] Decision Under S.111 of the Data Protection Act 2018 and for the Purposes of Article 60 of the General Data Protection Regulation (EU) 2016/679 (GDPR). DPC Case Reference: IN-19-1-1. Page 6.
[58] Decision Under S.111 of the Data Protection Act 2018 and for the Purposes of Article 60 of the General Data Protection Regulation (EU) 2016/679 (GDPR). DPC Case Reference: IN-19-1-1. Page 9.

is directly informed by its processor, but when it reasonably should have been aware of the breach. This interpretation reinforces the controller's accountability and ensures compliance with GDPR requirements.

In this specific incident with Twitter, its processor, Twitter Inc., identified the issue as a potential personal data breach on 3 January 2019. The DPC concluded that Twitter should have been made aware of the breach from that date rather than 7 January 2019, when actually became aware. This delay was due to the "*ineffectiveness of the process (...) and/or failure by Twitter Inc. staff to follow its incident management process*".[59] The latter was admitted by Twitter.

Since Twitter failed to notify the DPC within the 72-hour window – waiting until 8 January 2019 – its actions were deemed non-compliant per Article 33(1) of the GDPR.

With regards to paragraph 5, the DPC also concluded that Twitter failed to comply with its obligation to properly document the data breach. The documentation provided by Twitter was insufficient to allow the DPC to verify compliance with Article 33 requirements, as it lacked key details, such as how the breach was identified, the risk assessment process, and the timeline of events. The records submitted were general internal reports and communications related to incident management, rather than a specific and comprehensive record of the personal data breach.

Furthermore, the inquiry revealed that Twitter's documentation deficiencies required multiple follow-up queries to clarify the facts surrounding the breach, indicating that the records were not comprehensive or sufficient on their own. The DPC found that Twitter did not maintain adequate documentation, failing to demonstrate compliance with Article 33(5) of the GDPR.

Twitter believed that its documentation met the requirements of Article 33(5) of the GDPR and that the DPC was incorrectly interpreting the concept of 'controller awareness'.

As previously mentioned, an administrative fine of 450.000 EUR was imposed on Twitter. The DPC considered the nature, gravity, duration of the infringements and the mitigation actions[60] in determining the amount, pursuant to Article 83 of the GDPR. The DPA affirmed that the fine was proportionate to the infringement and emphasized the importance of

[59] Decision Under S.111 of the Data Protection Act 2018 and for the Purposes of Article 60 of the General Data Protection Regulation (EU) 2016/679 (GDPR). DPC Case Reference: IN-19-1-1. Page 88.
[60] Despite Twitter taking actions to remedy the underlying bug, these actions were not considered a significant mitigating factor in relation to the infringements of Article 33 of the GPDR.

dissuading similar non-compliance in the future, especially with regard to Article 33 obligations, and cautioned that future infringements could lead to more severe penalties.[61]

2.5.2. AP v. Booking.com

In 10 December 2020, the AP enforced an administrative fine of 475.000 EUR on Booking.com for failing to report a personal data breach within the legal required timeframe imposed by Article 33(1) of the GDPR.[62]

On 7 February 2019, Booking.com reported a personal data breach to the AP, following the discovery of unauthorized access to their reservation system (Extranet). An unknown third party had impersonated Booking.com employees and obtained access to customer reservation data through accommodation providers. This incident was labeled as social engineering by the AP, since it was non-technical.

This incident affected more than 4.000 individuals and the compromised data included customer names, addresses and phone numbers and booking details. The credit card information of almost 300 individuals was also compromised. These individuals were located in several Member States, but the AP determined it was competent to act as the lead DPA because Booking.com is headquartered in Amsterdam.

Despite the fact that Booking.com only notified AP on 7 February 2019, the Dutch DPA concluded that Booking.com was aware of the breach by 13 January 2019, based on multiple reports from accommodation providers. In light of this, the AP determined that Booking.com had sufficient knowledge of the incident and violated the 72-hour limit established by Article 33(1) of GDPR by notifying 22 days later.

Booking.com rejected this accusation and stated that only became aware of breach on 4 February 2019. It also defended that the breach was not caused by its systems. Additionally, Booking.com affirmed that the accommodation providers are also controllers for customers whose data is available through Extranet.

In light of this arguments, the AP did not accept this understanding and declared that Booking.com did not follow internal protocol to escalate the incident immediately to the security team, which was only notified on 31 January 2019, if it became aware of a security threat. In light of this, Booking.com should have, therefore, detected the obligation to inform AP. Failure to inform the security team is not a reason for delaying the notification process.

[61] Decision Under S.111 of the Data Protection Act 2018 and for the Purposes of Article 60 of the General Data Protection Regulation (EU) 2016/679 (GDPR). DPC Case Reference: IN-19-1-1. Pages 181 and 182.
[62] Decision of the AP against Booking.com, from 10 December 2020.

Moreover, the AP furthermore settled that Booking.com was the sole data controller, as it determined the purpose and means of processing the data, was the responsible party for Extranet and notified the AP about the breach alone.

Booking.com's failure to act promptly resulted in an unreasonable delay, increasing the risk of financial and identity fraud for affected customers, who lost control over their data.

Thus, the administrative fine imposed by AP considered several factors,[63] such as the severity of the breach, extent of the delay, risk to individuals and the mitigation actions[64] implemented by Booking.com, as laid out by Article 83 of the GDPR. The AP considered this fine was proportionate to the offense and within Booking.com's financial capability. Booking.com did not contest.

2.5.3. UODO v. Santander Bank Polska

In November 2018, a courier company was transporting a package of bank documents for Santander Bank Polska when the package was stolen. The package was later found discarded. The documents contained personal data from 158 bank clients. The bank learned about the incident on 24 November 2018 after one of its internal units found the reports online.

The compromised data included a wide range of personal information, such as names, dates of birth, bank account numbers, addresses, national identification numbers, email addresses, usernames and passwords, salary and asset information, phone numbers, loans and insurance policies.[65]

The bank did not report the breach to UODO or notified the affected data subjects, because it assessed the risk of the breach as low. The bank based its low-risk assessment on the fact that the package was found by one person, that no documents were missing, and the person who found the documents claimed not to have copied them.

The UODO learned about the breach through an online article on 23 August 2022. The DPA requested an explanation from the bank on 25 August 2022. After receiving clarifications from the bank, the UODO started an inquiry on 8 December 2022 against the bank for violations of the GDPR.

[63] See Article 83 of the GDPR.
[64] The fine was first set at 525.000 EUR, but it was reduced by 50.000 EUR because of the measures taken by Booking.com to mitigate damages, such as informing the data subjects about the incident.
[65] Decision of the UODO against Santander Bank Polska, from 12 March 2024. Case Reference: DKN.5131.59.2022

The UODO found that Santander Bank Polska violated Article 33(1) of the GDPR by failing to report the data breach to the DPA within 72 hours of becoming aware of it. The bank also violated Article 34(1) by failing to notify the affected data subjects without undue delay.

On 12 March 2024, the UODO issued a decision fining Santander Bank Polska 1.440.549 PLN[66] for the violations. The decision also ordered the bank to notify the affected individuals about the breach within three days of receiving the decision, including a description of the incident, contact information for the data protection officer, potential consequences of the breach and measures taken to mitigate risk.[67]

The UODO determined that the bank failed to adequately assess the risk of the personal data breach, which should have been evaluated from the perspective of the affected individuals. The DPA took into consideration the conditions established by Article 83 of the GDPR, such as the severity of the breach, the type of data compromised, and the potential harm to the data subjects, since there was a risk of identity theft and financial fraud. Similar to the DPC v. Twitter decision, the UODO determined that the imposed administrative fine was proportionate and aimed at deterring future violations.

2.5.4. Critical reflection

The cases of DPC v. Twitter, AP v. Booking.com, and UODO v. Santander Bank Polska collectively reveal significant weaknesses in the enforcement and practical application of Article 33 of the GDPR. While the 72-hour notification requirement and documentation obligations are well established, their interpretation and implementation in real-world scenarios remain fragmented and inconsistent across jurisdictions. In each case, the controllers failed to notify the DPA within the required timeframe, and in some cases did not notify affected individuals at all. These failures reflect not only organizational shortcomings, but also regulatory ambiguity and structural limitations in GDPR enforcement.

One of the central issues across all three cases is the problematic interpretation of ‘awareness’ under Article 33(1) of the GDPR. Both Twitter and Booking.com relied on internal procedural constraints and shifting definitions of responsibility to argue that their notification obligations had not yet been triggered. Twitter cited a failure to escalate the breach internally to the DPO, while Booking.com emphasized the lack of immediate awareness within its security team. In Santander’s case, the bank unilaterally determined that the breach posed a

[66] 326.000 EUR according to the GDPR Enforcement Tracker.
[67] Decision of the UODO against Santander Bank Polska, from 12 March 2024. Case Reference: DKN.5131.59.2022

low risk, bypassing both the DPA and the affected data subjects entirely. These justifications – however flawed – highlight a systemic ambiguity: when exactly does 'awareness' begin, and who within a corporate structure must possess that awareness in order for the time limit in Article 33 to start counting?

The current regulatory framework leaves this crucial concept under-defined. The GDPR offers no specific operational thresholds for 'awareness', leaving companies to apply their own interpretations, often in ways that downplay urgency or shift responsibility.[68] DPA's, while correct in their *ex-post* assessments, are reacting to failures that should have been prevented through clearer, binding interpretive guidance. This not only weakens enforcement, but also introduces regulatory asymmetry, as different DPA's adopt varying thresholds and tolerances for delay, further undermining the consistency the GDPR sought to achieve.[69]

In all three cases, internal escalation failures played a pivotal role. These failures are not merely technical oversights, but demonstrate that many organizations still lack a culture of data protection and proactive compliance. In Twitter's case, staff failed to follow the incident response process. Booking.com did not escalate the incident for weeks. Santander didn't notify the Polish DPA at all, rationalizing its decision with an unverified belief that no harm would result. These patterns suggest that the accountability principle of the GDPR, while legally entrenched, has not been internalized in operational practice. Organizations are still approaching personal data breach notification as a reactive obligation, rather than a fundamental part of responsible data governance.

The enforcement response from the DPA's, although legally justified, is also open to critique. All three fines were relatively modest—especially in the cases of Twitter and Booking.com—considering the global scale and revenue of these companies. While the DPA's referenced Article 83(2) and claimed that fines were proportionate, the actual financial impact on the controllers was minimal. These penalties risk being perceived as a cost of doing business, especially for large multinationals, which undermines the dissuasive function that administrative fines are meant to serve. Without sharper enforcement tools or higher financial stakes, companies may continue to treat breaches with insufficient urgency.[70]

[68] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026
[69] Golla, S. (2017). Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR. *JIPITEC*, 8(1), 70–78. https://www.jipitec.eu/issues/jipitec-8-1-2017/4533/JIPITEC_8_1_2017_Golla.pdf
[70] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026

Santander's case introduces a further, more troubling dimension: regulatory blind spots. The fact that the UODO only became aware of the breach four years after it occurred—and through a media article—raises concerns about how many other unreported breaches may go undetected. Article 58(1)(b) gives DPAs the power to conduct audits and investigations, yet this power is often underutilized due to resource constraints, lack of coordination, or risk-averse enforcement strategies.[71] The GDPR's reactive enforcement model assumes transparency and self-reporting from controllers. But as these cases show, this assumption is often misplaced.

Taken together, these cases point to a clear conclusion: Article 33, while foundational to the GDPR's vision of accountability, is not functioning as effectively as intended. The reliance on internal assessments, the ambiguity of controller 'awareness', and the weak deterrent power of fines all contribute to a landscape where late, incomplete, or absent personal data breach notifications are still common – even among major organizations with substantial compliance resources.

[71] Golla, S. (2017). Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR. *JIPITEC*, 8(1), 70–78. https://www.jipitec.eu/issues/jipitec-8-1-2017/4533/JIPITEC_8_1_2017_Golla.pdf

3. Article 33 of the GDPR

3.1. The process of notifying a personal data breach

Before we start to discuss the effectiveness of Article 33 of the GDPR, it is crucial to understand the process of notifying a personal data breach.

The first questions we have to ask are – what should be done in the event of a personal data breach? And when should the competent DPA be notified? Article 33(1) of the GPDR gives us an answer to both questions by stating that "*in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*".[72]

The process of notifying a personal data breach aims to guarantee transparency and accountability in the management of these security incidents. Although each breach is unique, with its own specificities, the notification process generally follows a set of common steps.

The first step is identifying the breach, which involves strategic stakeholders, such as the controller, who maintains the responsibility for the safeguarding of personal data breach; the processor, who processes personal data on the controller's behalf and is, therefore, required to notify the controller of any personal data breaches; the sub-processor, which processes personal data on behalf of the processor; and the data protection officer (hereinafter referred to as 'DPO'), who is responsible for overseeing all matters related to data protection.[73]

As Article 33(1) established, the controller must notify the personal data breach to the competent DPA with as little delay as possible, and, if possible, no later than 72 hours after becoming aware of it. The controllers' awareness has raised some questions, particularly when they can be deemed to have gained 'awareness' of the breach. According to the EDPB, controllers are considered aware of a personal data breach when they have a reasonable level of assurance that a security incident has taken place and that personal data breach has been exposed.[74]

[72] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[73] European Data Protection Board. *Guidelines on personal data breach notification for the European Union Institutions and Bodies*. Adopted 7 December 2018. Page 15.
[74] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 11.

The awareness of the controller will depend on the circumstances of breach. As mentioned beforehand, each personal data breach has a distinct nature – whereas some are quickly identifiable, others are not.

Despite this, the EDPB defends that the focus must be on the prompt action, and not on the awareness of the controller.[75] Which goes in line with the GDPR, which states that all appropriate technological protection and organizational measures must be implemented to quickly determine if a personal data breach has occurred and to promptly inform the competent SA.[76]

In light of this, controllers are therefore obliged to have measures in place to detect breaches in a timely manner, so they can take the necessary actions. It is also crucial that upon detecting a breach, it is reported to the appropriate person or persons responsible for handling these incidents to ensure it is address, proving the existence of the breach and, consequently, carrying out a risk assessment, and, if necessary, communicated to the competent DPA in compliance with Article 33 of the GDPR.

3.1.1. Controllers and processors

The controller can itself detect a personal data breach or can be informed of it by a data subject, a media organization, or by any processors that uses, for example. The controller, in addition to the technical and organizational measures required by Article 32 of the GDPR, must have the appropriate arrangements in place with the processors it uses.

If any of aforementioned parties alert the controller of a potential personal data breach, or itself detects an incident, it may initiate a brief period of investigation to determine whether or not there has been a breach. During this period, the controller cannot be considered as 'aware'. Once it has "*a reasonable degree of certainty*"[77] that a personal data breach occurred, it must notify the competent DPA without undue delay and within a maximum of 72 hours, fulfilling the obligation laid down in Article 33(1) of the GDPR.

In the cases where the controllers use processors, it is important to keep in mind that the first ones hold ultimate responsibility for the safeguarding of personal data; however, the processor plays a crucial part in helping the controller fulfill its obligations, including personal

[75] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 11.
[76] See Recital 87.
[77] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 11.

data breach notification.[78] This goes in line with Article 28(3)(f) of the GDPR, which stipulates that the processor must assist "*the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor*".[79]

In light of this, Article 33(2) of the GDPR lays down that the "*processor shall notify the controller without undue delay after becoming aware of a personal data breach*".[80] The GDPR does not specify an exact time limit for a processor to inform the controller of a breach. Nevertheless, the EDPB advocates that processors should promptly notify controllers, as this will help the latter to comply with the obligation laid down in Article 33(1) of the GDPR and report the breach within the stipulated timeframe.[81]

So, the processor's obligation is simply to notify the controller that a breach has occurred. The processor does not need to assess the risk resulting from the incident; this assessment is the responsibility of the controller. This helps the controller determining if the breach needs to be reported to the competent DPA under Article 33(1) of the GDPR. In addition to this, the controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts.[82]

Previously, we discussed the controllers' awareness of the breach. Further to what was said, the controller is deemed 'aware' once the processor has notified them of the incident.[83] Since Article 28(3) of the GDPR establishes that the "*processing by a processor shall be governed by a contract or other legal act*",[84] the contract between the controller and the processor can include provisions for early notification by the processor,[85] such as notifying the controller within 24 hours after becoming aware of the incident, supplying relevant details

[78] Lambrinoudakis, C. (2018). The General Data Protection Regulation (GDPR) ERA: Ten Steps for Compliance of Data Processors and Data Controllers. In *Lecture notes in computer science* (pp. 3–8). https://doi.org/10.1007/978-3-319-98385-1_1

[79] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

[80] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

[81] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 14.

[82] E.g., if the controller possesses copies or backups of personal data destroyed in the breach.

[83] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 13.

[84] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

[85] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 14.

about the breach and conducting a risk assessment, for example, thereby aiding the controller in meeting its obligation to report to the competent DPA within 72 hours.

3.1.2. Risk assessment

The next step is risk assessment. As mentioned beforehand, each personal data breach is unique – while some are quickly identifiable, others may take longer to detect. This highlights the urgency of containing the incident and assessing the risk in order to identify the severity and potential impact of the breach. Thus, assessing the risk also helps the controller to take the necessary and effective steps to control the incident and to decide whether or not to notify the competent DPA.

As discussed in the previous chapter, there is a risk when a personal data breach is likely to result in physical, material or non-material damage for the affected data subjects.

Considering this, the WP29 recommends conducting the risk assessment by evaluating the following specificities.[86] The first one is the type of breach, i.e. whether there has been a breach of confidentiality, availability or integrity.

The second one is the nature, sensitivity and volume of personal data. That is, to understand whether there are any special categories of personal data, since these represent a greater risk to data subjects if disclosed in a breach, or simply to understand the sensitivity of the data compromised. For example, the disclosure of a name is unlikely to cause harm to the data subject. However, a combination of a name, address and credit card information, for example, can lead to identity theft and financial fraud, which could represent an enormous risk to a data subject. So, we can conclude the combination of personal data can represent a greater risk than an individual piece of data. In the wake of this, a small amount of compromised sensitive data can mean a high risk as large volumes of data.

The third one is the ease of identification of individuals. In other words, assessing how easy it is to identify individuals from the compromised data or match it with other information. One way to overcome this is to implement data pseudonymization,[87] as this will reduce the possibility of data subjects being identified in a personal data breach.

The fourth one is the severity of consequences for individuals, which means that the controller must always consider the potential consequences of a personal data breach for the data subjects.

[86] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 24.
[87] See Article 4(5) of the GDPR.

The fifth one is the special characteristics of the individual. It is important to consider whether a personal data breach involves children or vulnerable minorities, for example, since a personal data breach could put them at even greater risk.

The sixth one is the special characteristics of the controller. It is also imperative to take into account the nature of the controller. Following on from the previous point, if the controller is a NGO that deals with children at risk, a personal data breach could mean a tremendous risk for these children.

And finally, the seventh one is the number of affected individuals. As we know, a breach can affect one individual or thousands of them. There is no 'in between'. It is clear that a personal data breach involving thousands of people will have a major impact. But, as said before, a breach involving sensitive data of one individual may also have a big impact. Therefore, the EDPB recommendation is always to consider the sensitive of the compromised data and the severity of the impact.[88]

3.1.3. Notification to the competent supervisory authority

After assessing the risk, the controller is left with two scenarios: if the personal data breach is likely to result in a risk to the rights and freedoms of data subjects, the controller must notify the incident to the competent DPA within 72 hours after becoming aware of it, and without undue delay, pursuant to Article 33(1) of the GDPR; conversely, if there is no risk, the notification to the competent SA is not necessary.

In the first scenario, the GDPR, on its Article 33(3), establishes that the notification shall at least the following details: (a) the nature of the breach, including, if possible, the categories and estimated number of affected data subjects and records; (b) the name and contact information of the DPO or another relevant contact point for further inquiries; (c) the potential consequences of the personal data breaches; and (d) the measures taken or planned by the controller to address the personal data breach, including any steps to mitigate its potential negative impact.[89]

By reading this paragraph, we quickly realize that the GDPR does not include the categories of data subjects or the types of personal data. Taking into consideration what was said in the previous subchapter regarding criteria to assess risk, the EDPB recommends that if

[88] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 26.
[89] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

the categories of data subjects or types of personal data suggest a risk of a potential consequence arising from the breach (like identity theft or financial fraud), it is crucial for the notification to highlight these specificities, as this aligns with the requirement to outline the potential consequences of the incident.[90]

On the contrary, if the controller does not have precise information at the moment, this should not be an obstacle to notify the authority in a timely manner. Meaning, if a company or an organization suffers a personal data breach and its extent is not yet known, the GDPR recognizes the possibility for the controller to notify in phases.

In light of this, Article 33(4) of the GDPR states that "*where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay*".[91] So, there is the possibility to provide further details about the breach if necessary.

The option to notify in phases is the GDPR's way of recognizing that controllers may not always have all the necessary information about a personal data breach within 72 hours of becoming aware of it. This is particularly relevant for highly complex security incidents, which are becoming more recurrent every day, and are harder to predict and contain, taking more time to scrutinize.

In such cases, the EDPB recommends that the controller informs the competent DPA at the time of the initial notification that all required information is not yet available and that it will provide further details at a later stage. Given this, the competent DPA should agree on how and when the additional information is to be provided.[92] This possibility is a reliable way to induce controllers to comply with notification obligations.

In the cases where the controller fails to comply with the 72-hour deadline imposed by Article 33(1) of the GDPR, the notification must be accompanied by the reasons that led to the delay. Once again, this is the GDPR acknowledging that controllers may not always have all the necessary information about a personal data breach within 72 hours of becoming aware of it and that late notifications can be recognized and tolerated. However, this must not be a regular occurrence.

---

[90] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 15.

[91] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

[92] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 15.

3.1.4. Record keeping

Pursuant to Article 33(5) of the GDPR, "*the controller shall document any personal data breaches, compromising the facts relating to the personal data breach, its effects and the remedial action taken*".[93] When the paragraph mentions 'any' it means that controllers are obliged to document all personal data breaches, regardless of whether or not these needs to be notified to the competent DPA.

This obligation is in line with the principle of accountability laid out on Article 5(2) of the GDPR, which holds controllers responsible for ensuring and demonstrating compliance with the principles established on paragraph 1. Paragraph 1(f) mandates that personal data must be processed securely, protecting it against unauthorized or unlawful access, accidental loss, destruction or damage, through the appropriate technical and organizational measures.[94]

Therefore, the controller must maintain documentation of all breaches in order to ensure compliance with Article 33(5) of the GDPR, or with the principle of accountability.[95] The internal register of breaches is a way for the DPA to verify compliance, as set by the final part of the Article previously mentioned.

If the controller, after the risk assessment, decides not to notify the competent DPA of the personal data breach, it should record the justification, including the reasons for considering the breach is unlikely to result in a risk to the rights and freedoms of data subjects. And in the cases where the controller actually notifies the personal data breach to the competent DPA, but fails to do so within the stipulated period, this documentation can help to prove whether the delay is justifiable and not unreasonable.

The EDPB recommends that both controllers and processors should have a documented notification procedure, as it can help to take appropriate action in the event of a personal data breach.[96]

[93] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[94] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[95] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 26.
[96] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 27.

3.2. Communication to the data subjects

After analyzing the process of notifying a personal data breach to a DPA, only the last step remains to be assessed: the communication to the data subjects.

Article 34(1) of the GDPR determines that the controller must inform data subjects without unnecessary delay if a personal data breach is likely to result in a high risk to their rights and freedoms.[97]

Unlike Article 33(1), there is no stipulated timeframe for communication to data subjects in the event of a personal data breach. However, the EDPB recommends that this communication must be made "*as soon as possible*".[98] Recital 86 of the GDPR goes in line with this, when it states that the "*communications to data subjects should be made as soon as reasonably feasible*".[99] This enables individuals to take the necessary actions to protect themselves from the adverse consequences of the incident.

Case law further supports this interpretation. In DKN.5131.33.2021, the UODO, the Polish DPA, investigated a personal data breach involving 10,500 data subjects at Santander Bank Polska caused by a former employee who, despite their contract termination, retained unauthorized access to the Electronic Platform of Services of the Social Insurance Institution. Over several logins, the employee accessed names, addresses, national identification numbers, and sick leave details. The bank failed to notify the affected individuals, prompting an administrative proceeding by the UODO.[100]

The Polish DPA found that the breach compromised data confidentiality and posed as a high risk to data subjects' rights. Citing Articles 34 and 12 of the GDPR, it ruled that the bank should have informed the affected data subjects. Consequently, the UODO fined Santander Bank Polska 545,748 PLN[101] and ordered it to notify all affected data subjects. The DPA emphasized that when a personal data breach presents a high risk to the rights and freedoms of data subjects, controllers must notify data subjects without undue delay and as soon as possible.

[97] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[98] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 20.
[99] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[100] Decision of the UODO against Santander Bank Polska, from 19 January 2022. Case Reference: DKN.5131.33.2021
[101] Approximately 120.000 EUR, according to GDPR Enforcement Tracker.

According to Article 34(2) of the GDPR, the controller must ensure that the communication to the data subject, as mentioned in paragraph 1 of the previously mentioned article, clearly and simply explains the nature of the personal data breach. It must also include the information specified in subparagraphs (b), (c) and (d) of Article 33(1), such as (i) the contact details of the DPO; (ii) a description of the consequences of the personal data breach; and (iii) a description of the measures implemented or proposed to be implemented by the controller to address the breach, including, if applicable, actions to mitigate potential negative effects. In addition to this, the controllers may also provide additional information.[102]

When a personal data breach occurs, the affected data subjects should generally be informed directly unless doing so would require disproportionate effort. In these cases, a public communication or a similar method can be used as an alternative.[103]

These notifications should be sent through dedicated messages, separate from other communications, such as newsletters, and should use transparent methods, like an email or website notices. Communications should avoid compromised channels and must be accessible in alternative formats and languages, if necessary. The EDPB recommends a method that "*maximizes the chance of properly communicating information to all affected individuals*".[104] Despite this, and depending on the situation, multiple communication methods may be required to ensure information reaches all affected individuals effectively. The controllers may consult the competent SA to determine the most appropriate messaging and delivery methods.

However, the communication to data subjects may be delayed if law enforcements advises that early disclosure could hinder investigations, but affected individuals must be informed promptly once permitted.[105] For instance, if the personal data breach is linked to a larger criminal activity, alerting the individuals too soon could warn the cyber attackers and obstruct the investigation.

Under Article 34(3) of the GDPR, notifying data subjects about a personal data breach is not required in specific situations. This applies if the controller has implemented and applied appropriate technical and organizational measures, such as encryption, making it unintelligible to unauthorized persons. Notification is also unnecessary if further measures have been taken

[102] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[103] See Article 34(3)(c) of the GDPR.
[104] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 21.
[105] See Recital 88 of the GDPR.

to eliminate the high risk to individuals' rights and freedoms or if the effort required to notify would be disproportionate.

Controllers must be able to demonstrate to the competent SA, pursuant to principle of accountability, that one or more of these conditions apply. Still, the DPA retains the right to mandate communication with affected individuals if it determines that the breach is likely to pose a high risk. If the DPA finds the decision not to notify data subjects unjustified, it may take enforcement action or impose sanctions.

3.3. Remedies and sanctions for non-compliance with personal data breach notifications

As discussed, controllers have a legal obligation to notify personal data breaches as outlined in Articles 33 and 34 of the GDPR. Failure to comply with these obligations can lead to significant sanctions.

A data subject who believes its personal data has been mishandled, has the right to file complaints with the relevant DPA under Article 77 of the GDPR, if it "*considers that the processing of personal data relating to him or her infringes this Regulation*".[106] Beyond these administrative complaints, data subjects also have the right to seek judicial remedies against controllers, as established in Article 79 of the GDPR. In addition, alternative dispute resolution mechanisms may also be available for individuals seeking remedies outside of formal legal proceedings.

Like mentioned above, non-compliance with personal data breach notification obligations can result in severe financial sanctions. According to Article 58(2)(i) of the GDPR, that determines the investigative powers for DPA's, these can "*impose an administrative fine pursuant to Article 83*".[107] These administrative fines,[108] according to Article 83(1) are supposed to be "*effective, proportionate and dissuasive*"[109], in order to ensure that the rules of the GDPR are properly enforced.[110] In paragraph 2 of the above-mentioned article, we can find

[106] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[107] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[108] See Recital 150 of the GDPR.
[109] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[110] See Recital 148 of the GDPR.

the criteria that must be taken into account when DPA's are deciding whether to impose an administrative fine and, consequently, when they are deciding on the amount of the fine. The criteria include the nature, gravity and duration of the infringement, if it was intentional or negligent, the actions taken by the controller, and others.

Article 83(4) of the GDPR states that the SA's can impose fines up to 10 million EUR or 2% of a company's total worldwide annual turnover, whichever is higher.[111] These substantial penalties, as mentioned beforehand, highlight the importance of ensuring proper notification procedures are in place are supposed to have a dissuasive effect.

While the GDPR establishes broad penalties for non-compliance, Article 84[112] allows Member States to implement additional penalties through domestic law, "*in particular for infringements which are not subject to administrative fines pursuant to Article 83*".[113] These additional penalties, like the administrative fines, must also be to be effective, proportionate and dissuasive.

3.4. The effectiveness of Article 33 of the GDPR

Despite the remedies and sanctions for non-compliance mentioned beforehand, it is evident that the current data protection framework may not be entirely effective in ensuring that all companies and organizations notify the competent DPA within 72 hours of becoming aware of a personal data breach. While Article 33 of the GDPR establishes a clear obligation for timely breach notification, the growing frequency and complexity of cyber threats make it increasingly difficult for companies to detect and assess personal data breaches within this timeframe. As a result, the current notification system is struggling to keep pace with the evolving threat landscape, leading to delays in notifying and potentially leaving data subjects exposed to harm for longer than necessary.

Given this, there are several factors that can explain the ineffectiveness of Article 33 of the GDPR, that we will further discuss in the following subchapters.

[111] In view of the amounts at stake, controllers are gradually considering obtaining a cyber insurance to cover the costs of security incidents and personal data breaches.
[112] See Recital 149 of the GDPR.
[113] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

3.4.1. The controllers and their failure to notify personal data breaches

When it comes to personal data breaches, the EU is facing a big challenge, which is inducing controllers to notify these incidents. And why is that? Because the disclosure of a personal data breach imposes administrative costs and poses significant risks to a company's reputation. The fear of reputational damage can deter companies from notifying personal data breaches, as short-term losses in market, individuals' loss of trust and potential legal liabilities may follow. And while some organizations recover with minimal long-term damage, others may face severe damages, including financial insolvency. Thus, many companies and organizations choose not to report personal data breaches to competent SA's, opting to handle the matter internally.

As discussed previously, the GDPR imposes significant sanctions for non-compliance with notification requirements. This can lead to two scenarios: under-deterrence and over-deterrence.[114]

Under-deterrence occurs when controllers perceive a low likelihood of detection and therefore decide not to report personal data breaches. The assumption is that if the probability of getting caught is low, the risk of a fine is outweighed by the costs of notifying. In these circumstances, companies and organizations tend to exhibit risk-seeking behavior to avoid or minimize losses, which means that, rather than complying with notification requirements, some prefer to gamble that their failure to report a personal data breach will go unnoticed.[115]

In contrast, over-deterrence happens when controllers, unsure of the exact legal thresholds for mandatory notification, report personal data breaches excessively to avoid administrative fines. This can result in the notification of breaches of security that pose little or no actual risks to data subjects. Over-notifying leads to notification fatigue and can create an administrative burden for the DPA's and divert resources from addressing genuinely harmful personal data breaches. It also imposes unnecessary costs on organizations that disclose breaches that may not have warranted notification. As a result, both companies and DPA's are overwhelmed with notifications that do not necessarily enhance data protection. Notification fatigue can also lead to data subjects paying less attention to reported personal data breaches

[114] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026. Page 1240-1241.

[115] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026. Page 1240-1241.

as the dissemination of information becomes less effective and, over time, all these incidents may be perceived as insignificant or irrelevant.[116]

On the other hand, high sanctions can be a potential incentive and enabler for organizations to avoid detecting personal data breaches altogether and, consequently, report them to the competent DPA. Taking into consideration what was said beforehand about the awareness of the controller, companies and organizations might deprioritize security measures to maintain plausible deniability of being aware of a personal data breach, thus avoiding the notification.

In light of this, we can conclude that the effectiveness of personal data breach notifications is influenced by how organizations perceive the risks and benefits of notifying. While high sanctions are intended to dissuade non-compliance, they can lead to counterproductive behaviors, such as excessive reporting, concealment of personal data breaches, or deliberate ignorance of these incidents.

Striking a balance between dissuasion and practicality is crucial to ensuring that data controllers take appropriate action when breaches occur while avoiding unnecessary burdens on companies and organizations and DPA's. As cyber threats continue to evolve, refining the notification process to encourage responsible disclosure without inducing fear-driven overcompliance or avoidance will be essential for the long-term success of the EU data protection framework.

3.4.2. The discrepancy between 'security incident' and 'personal data breach' in European data protection legislation

Most EU data protection laws, as previously stated, such as the GDPR, the Data Protection Law Enforcement Directive and the Data Protection Regulation for EU Institutions, defined personal data breaches as a 'breach of security'. However, there is an absence of a clear definition of the latter. So, what is the critical distinction between 'breach of security' and 'personal data breach'?

Beginning with 'personal data breaches', and as previously stated, most EU data protection laws define these as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data*

[116] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026. Page 1241-1242.

transmitted, stored or otherwise processed".[117] A personal data breach can involve, for example, the "*non-compliance of a technical or organizational security measure of data processing or an actual defeat of a security infrastructure accompanied by an adverse effect on personal data*".[118]

As far as 'breach of security' is concerned, and since there is an absence of a definition for this concept, we have to take a look at EU information security law, as there is an interplay between this term and 'security incident' across the current framework. Starting with the recent NIS 2,[119] this directive defines an 'incident', on its Article 6(6), as "*an event compromising the availability, authenticity, integrity or confidentiality of store, transmitted or processed data of the services offered by, or accessible via, network and information systems*".[120] This definition is actually a new introduction by NIS 2, as NIS, the predecessor, established on its Article 4(7) an 'incident' as "*any event having an actual adverse effect on the security of network and information systems*".[121] NIS 2 defines on Article 6(2) 'security of network and information systems' as "*the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of store, transmitted or processed data or of the services offered by, or accessible via, those network and information systems*".[122]

In light of this, we can conclude that the term 'breach of security' in EU data protection laws is generally similar to its usage in the context of EU information security laws.

However, we have to keep in mind what the WP29 said in order to understand the main difference between security incidents and personal data breaches. As previously said, despite all personal data breaches being considered security incidents, not all security incidents are

[117] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[118] Alunge, R. (2020). *Breach of security vs personal data breach: effect on EU data subject notification requirements*. International Data Privacy Law, 11(2), 163-181. https://doi.org/10.1093/idpl/ipaa021.
[119] This Directive came into force on 16 January 2023 and is an update from its predecessor, the NIS Directive. NIS 2 aims to strengthening cybersecurity across the EU Member States. These had until 17 October 17 2024 to transpose it into their national laws.
[120] 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).
[121] 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 network and information systems across the Union.
[122] 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).

considered personal data breaches.[123] Consequently, and looking at the definitions given above, we can conclude that the major difference between these the terms relies on the fact that a personal data breach requires an actual compromise of personal data, whereas a security incident does not.

Taking into account the above, it is safe to say that the current EU personal data breach notification process has significant limitations. One of them due is the narrow focus on personal data breaches, which essentially require both a breach of security and a resulting compromise of personal data. This approach overlooks security incidents that may pose a risk to data subjects, but do not immediately lead to a confirmed data compromise. As a result, incidents where security is breached, but personal data exposure cannot yet be determined, may fall outside the scope of notification requirements established by Article 33 of the GDPR. Given the increasing frequency and sophistication of cyberattacks, this gap in regulation could leave individuals vulnerable to harm while investigations are still ongoing. This approach may also delay necessary protective actions for data subjects and prevent them from the taking early precautions.

Additionally, the requirement to confirm a data compromise can lead to delays in notifying the personal data breach to the competent DPA, and consequently to the affected data subjects. Controllers must first conduct an investigation to establish whether personal data has been compromised before an incident is classified as a reportable breach of security. This process can be time-consuming, particularly in cases involving complex cyberattacks or refined intrusion methods. During this period, individuals remain unaware of potential risks to their personal data, limiting their ability to take protective measures, as a delayed notification can significantly increase the risk of financial fraud, identity theft and others.

By focusing solely on confirmed data compromise, the current EU data protection framework may also overlook the potential harm that a security incident itself can cause. A security incident does not need to result in immediate data exposure to pose as a risk to data subjects. Cyber attackers could exploit security vulnerabilities to access personal data at a later stage, or the incident could indicate systemic weaknesses that threaten ongoing data security. However, and under the current regulations, these risks are not always taken into account when determining whether notification to the competent DPA is necessary, which reduces the level of protection available to data subjects.

[123] European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023. Page 8.

Moreover, and as previously discussed, the notification obligations are only triggered once there is a reasonable degree of certainty that personal data has been affected, meaning that organizations may not feel an urgent need to address security vulnerabilities that pose a risk to the rights and freedoms to personal data breaches. This lack of immediate accountability can lead to delays in implementing stronger security measures or notifying the competent DPA, ultimately undermining overall data protection efforts. The concept of 'awareness of the controller' further complicates this issue. This means that some security incidents, especially those involving highly complex cyber threats, may go unreported for extended periods, as determining the extent of a compromise of personal data can be very challenging, further prolonging the notification process.

The GDPR, by requiring a confirmed compromise of personal data before triggering legal obligations, fails to compel companies and organizations to notify, thereby failing to adequately protect data subjects from security incidents that present real risks. The narrow definition of personal data breaches and the emphasis on certainty rather than potential harm leaves gaps in protection, potentially delaying critical notifications and risk mitigation efforts. A more proactive approach that considers security incidents as potential threats, even before personal data compromise if fully determined, would provide better safeguards in an increasingly digital and interconnected world.

3.4.3. Is the timeframe imposed by Article 33(1) adequate?

In addition to the narrow focus on personal data breaches, the timeframe imposed by Article 33 of the GDPR may also lead to its ineffectiveness. In order to understand this, it is important to take a look again to EU information security laws.

Article 23(1) of the NIS 2 Directive requires Member States to ensure that essential and important entities promptly notify their CSIRT (Computer Security Incident Response Team) or, where applicable, the competent authority of any incident that significantly affects their services, as outlined in paragraph 4. It also obliges these entities to inform service recipients without undue delay if an incident is likely to disrupt service provision.[124]

Paragraph 3 of the aforementioned article defines a significant incident as one that (i) has resulted in or has the potential to cause substantial operational disruption to services or

[124] 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).

financial loss for the affected entity, and (ii) has impacted or could impact other individuals or organizations by causing significant material or non-material harm.[125]

With regard to the period established for reporting to the competent authority, paragraph 4 of Article 23 of the NIS 2 Directive requires entities to issue an early warning without undue delay and no later than 24 hours after becoming aware of a significant incident. This warning should specify, if applicable, whether the incident is suspected to result from unlawful or malicious actions or may have cross-border implications. Similar to the GDPR, a full incident must be incident within 72 hours of detection, providing an initial assessment of the incident, including its severity, impact, and any available indicators of compromise.[126]

Given this structured two-step approach under the NIS 2 Directive, a similar framework could be considered for the GDPR to enhance the effectiveness of personal data breach notifications. Implementing a 24-hour requirement for an initial notification – focused on alerting the competent DPA about the mere occurrence of a personal data breach – followed by a more detailed report within 72 hours, could significantly improve timely response and risk mitigation.

Under the current framework, Article 33(1) establishes that controllers must notify DPA's without undue delay and, if possible, within 72 hours of becoming aware of the breach.[127] However, the increasing sophistication and volume of cyber threats pose challenges to identifying and assessing personal data breaches within this timeframe, as it can take longer to detect and fully analyze them.

By requiring an initial notification with 24 hours of detection, organizations could immediately alert authorities to a potential personal data breach without needing to complete a full forensic investigation within 72 hours. This early warning system would enable authorities to take preliminary steps, such as advising on mitigation measures. Additionally, it would help prevent unnecessary delays in responding to high-risk breaches, which could otherwise leave data subjects exposed to long-term risks. The final notification at 72 hours could then provide

[125] 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).
[126] 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).
[127] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

a more detailed assessment, including the severity of the breach, affected individuals, and remedial measures taken.[128]

Thus, the current GDPR notification framework may not be fully effective in addressing the realities of modern cybersecurity threats. Its rigid requirement for full notification within 72 hours does not always account for the time needed to uncover the full extent of an attack, potentially leading to incomplete or inaccurate reports. Furthermore, the lack of an early warning mechanism means that DPA's may only become aware of a personal data breach once significant damage has already occurred. This two-tiered approach would align the GDPR more closely with evolving cybersecurity challenges, by harmonizing the data protection framework with the information security framework at EU level, while ensuring that organizations do not delay reporting due to uncertainties about the breach's full scope. It would also acknowledge the reality that, in many cases, forensic investigations take longer than 72 hours to complete, particularly for complex cyberattacks involving sophisticated methods. By implementing an early warning mechanism, authorities could proactively monitor emerging threats, while affected data subjects could take protective measures sooner. This approach may also induce controllers to notify more swiftly, as they would be less concerned about the immediate requirement for a fully completed investigation, by allowing them to fulfill their obligations more quickly and with less risk of non-compliance, whilst not fearing sanctions and reputational damage.

This modification to the GDPR could improve the overall effectiveness of breach notifications, ensuring that regulatory responses are both timely and informed, while also adapting to the modern cybersecurity landscape.

[128] Alunge, R. (2020). *Breach of security vs personal data breach: effect on EU data subject notification requirements*. International Data Privacy Law, 11(2), 163-181. https://doi.org/10.1093/idpl/ipaa021.

4. Going forward – what can be improved in order for organizations to comply with Article 33 of the GDPR?

In an increasingly digital world, the protection of personal data has become a key concern for companies and organizations. Personal data breaches can have serious consequences, including financial losses, reputational damage and legal liabilities. Consequently, organizations must take a proactive approach when it comes to handle with personal data breaches, ensuring compliance with legal requirements and minimizing potential damage.

As studied in the last chapter, the current EU data breach notification may fall short of ensuring timely and effective compliance with Article 33 of the GDPR. The regulation's requirement for a confirmed compromise of personal data before triggering legal obligations creates significant delays in reporting, ultimately failing to provide adequate protection for data subjects. By emphasizing certainty over potential harm, the GDPR's notification mechanism leaves critical gaps in the early detection and mitigation of breaches of security. This rigid approach not only hinders proactive responses, but also increases the risk of delayed notifications, allowing threats to escalate before appropriate action can be taken.

Moreover, the GDPR's strict 72-hour notification requirement does not always align with the complexities of modern cybersecurity threats. Companies and organizations often struggle to determine the full scope of an cyberattack within this timeframe, leading to either incomplete or inaccurate reports. The absence of an early warning system means that DPA's are frequently made aware of breaches only after substantial harm has occurred. Implementing a more flexible and proactive approach – such as a two-tiered notification, as established in the NIS 2 Directive – could better align the current data protection framework with the evolving cybersecurity challenges. By introducing an early mechanism, organizations would be encouraged to report incidents sooner, without the fear of administrative fines. This would enable DPA's to monitor emerging threats more effectively while allowing affected individuals to take timely protective measures. Ultimately, refining Article 33 of the GDPR to accommodate the realities of forensic investigations and cyber incident response would not only improve compliance rates, but also enhance overall data security across the EU digital landscape.

Thus, and until the EU data protection framework takes the previously mentioned factors into consideration, this chapter explores good practices and structured procedures for effectively managing notifications and communications related to personal data breaches, with

an emphasis on prevention, response planning, risk management and regulatory compliance. By being aware that the human and financial resources available to micro or large corporations vary significantly, influencing their approach to reporting personal data breaches, this chapter also aims to outline a set of best practices applicable to all entities, regardless of their size.

4.1. Good practices

A number of good practices can facilitate the process of notifying personal data breaches for controllers. However, these practices should not be confined solely to the act of notifying SA's. An effective notification requires a comprehensive approach that includes risk assessment, a clear description of the affected data and data subject categories, and a solid understanding of fundamental principles, such as implementing appropriate security measures, for example.[129]

To meet the current GDPR's notification deadlines and requirements, as analyzed in Chapter 3 of this dissertation, controllers and processors must fully understand their responsibilities and implement the necessary technical and organizational measures for the personal data they process. So, these good practices extended beyond merely following a breach notification procedure; it involves implementing the appropriate security measures and establishing clear internal and external communications chains from the beginning of the processing.

4.1.1. Establishing a comprehensive data protection policy

A well-defined data protection policy serves as the foundation for ensuring compliance, safeguarding personal data, and maintaining operational security. This policy must be personalized to the company or organization's unique structure, activities, and potential risks.[130] In view of this, Article 24(2) of the GDPR, that establishes the responsibility of the controller, mentions that the implementation of appropriate technical and organizational

[129] Esayas, S. Y. (2015). Breach notification requirements under the European Union Legal Framework: convergence, conflicts and complexity in compliance. *SSRN Electronic Journal.* https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2746834_code2035392.pdf?abstractid=2746834&mirid=1&type=2

[130] Julakanti, S. R., Kiranmayee Sattiraju, N. S., & Julakanti, R. (2025). Data Protection through Governance Frameworks. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2502.10404

measures by the controller, stipulated in the previous paragraph, shall also "*include the implementation of appropriate data protection policies*".[131]

In order to be effective, the policy should clearly outline its purpose, providing employees with an understanding of why specific data protection measures are in place. It must also define responsibilities, ensuring that each member of the organization understands their role in handling personal data and maintaining compliance.[132] Clear terminology should be used to eliminate ambiguity, and any exceptions to the policy should be explicitly defined.

The scope of the policy should be explicitly stated, detailing how different classifications of personal data will be processed and protected.[133] Furthermore, and to reinforce adherence, the data protection policy should establish clear consequences for non-compliance. In light of this, companies must ensure that their policies align with the obligations established in the GDPR.

Another key aspect of an effective data protection policy is incident communication, which defines how personal data breaches should be reported internally and externally.[134] This includes notification protocols for DPA's and affected data subjects, in order to comply with the obligations established in Articles 33 and 34 of the GDPR.

The policy must undergo review and monitoring, making sure it remains up to date with evolving threats and regulatory changes. Organizations should schedule a review date at least annually to reassess its effectiveness. The approval date of the policy must be documented as well.[135]

To ensure accountability, the authorship and the responsible body for enforcing the policy should be identified. Ideally, a DPO should be appointed to oversee implementation and compliance.

According to Article 37(1) of the GDPR, a controller shall designate a DPO in the following cases: (i) when the processing is conducted by a public authority or body, excluding courts acting in their judicial role; (ii) when the primary activities of the controller or processor

[131] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[132] Julakanti, S. R., Kiranmayee Sattiraju, N. S., & Julakanti, R. (2025). Data Protection through Governance Frameworks. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2502.10404
[133] Julakanti, S. R., Kiranmayee Sattiraju, N. S., & Julakanti, R. (2025). Data Protection through Governance Frameworks. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2502.10404
[134] Julakanti, S. R., Kiranmayee Sattiraju, N. S., & Julakanti, R. (2025). Data Protection through Governance Frameworks. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2502.10404
[135] Julakanti, S. R., Kiranmayee Sattiraju, N. S., & Julakanti, R. (2025). Data Protection through Governance Frameworks. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2502.10404

involve processing operations that, due to their nature, scope, and/or purpose, demands frequent and systematic monitoring on a large scale of data subjects; and (iii) when the main activities of the controller or processor involve large-scale processing of special categories of data as defined in Article 9, or personal data related to criminal convictions and offences as outlined in Article 10.[136]

Although the GPDR only established the appointment of a DPO in those three cases, companies and organizations can still appoint one. And that would be beneficial, since appointing a DPO is a strategic decision that enhances an organization's liability to manage data protection responsibilities, since it performs a crucial role in shaping the data protection policy, ensuring GDPR compliance,[137] and guiding the company in responding to personal data breaches. Their expertise helps controllers, and processors, navigate complex regulatory requirements while maintaining robust security measures.

4.1.2. Utilizing codes of conduct and certification mechanisms

Companies and organizations should also leverage codes of conduct and certification mechanisms, as outlined in Articles 40 and 41 of the GDPR to standardize data protection and security. These mechanisms help bridge regulatory differences, ensuring that minimum security requirements are consistently applied to all organizational structures. By going beyond basic legal obligations, certification provides additional guarantees of security and compliance, strengthening the organization's ability to protect personal data.[138]

Certification and codes of conduct serve as valuable tools for evaluating a company's security posture. They enable the analysis and assessment of risks, the implementation and definition of an information security management system (hereinafter 'ISMS'). Additionally, certification can define clear security objectives, propose concrete risk management strategies, and establish roles, responsibilities, and technologies necessary for the protection of personal data. This structured approach supports the effective implementation of security controls and also helps to mitigate potential damage from security incidents.

Certification also offers several key benefits for organizations seeking to enhance their information security practices, which is fundamental, since data protection and information

[136] Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.
[137] See Article 38 of the GDPR, which defines the position of the DPO.
[138] European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*. 2018 edition. Page 183.

security are interrelated.[139] By formalizing security processes through structured documentation, it ensures consistency and clarity in how data protection measures are implemented and maintained. It provides a systematic approach to identifying and managing risks, allowing companies and organizations to proactively address vulnerabilities and strengthen their security attitude. Furthermore, it helps clarify regulatory requirements, particularly for businesses engaged in contractual agreements that demand compliance with rigorous data protection standards – from personal experience, this is very common in the field of IT consultancy. This structured framework not only improves security resilience, but also fosters trust among stakeholders and regulatory authorities.

One of the most important international certifications is the ISO/IEC[140] 27000 family, which covers a wide number of standards on information security. Inside this family, the most known standard is the ISO/IEC 27001.

This standard establishes a global reference model for implementing and improving an ISMS, ensuring the confidentiality, integrity and availability of data through structured risk management. The standard outlines the "*requirements for developing, implementing, maintaining, and continuously improving*"[141] an ISMS.

Although ISO/IEC 27001 does not explicitly mandate this four-phase approach, companies and organizations often follow this structured process. This begins with defining the organization's context, determining the ISMS scope, and setting objectives. It then moves to implementation, involving risk assessment, the application of security controls,[142] resource management, and ensuring staff competence. Performance evaluation follows, requiring the organization to monitor, measure, analyze, and assess the ISMS. Lastly, and after this three steps, the process emphasizes the continual improvement by identifying non-conformities, implementing corrective actions, and enhancing security measures to adapt to evolving threats.[143]

Besides the ISO/IEC 27001, there is another relevant standard – the ISO/IEC 27035. This standard comprehends the management of information security vulnerabilities and

[139] Testimony from a Cybersecurity Officer, interviewed for the purpose of writing this dissertation.
[140] Abbreviation for International Organization of Standardization and International Electrotechnical Commission, respectively. The standards are jointly published.
[141] ISO/IEC 27001:2023 – *Information security, cybersecurity and privacy protection – Information security management systems - Requirements*
[142] For security controls and best practices, there is ISO/IEC 27002. This one is not a certification, but a guideline that supports the ISO/IEC 27001 implementation.
[143] ISO/IEC 27001:2023 – *Information security, cybersecurity and privacy protection – Information security management systems - Requirements*

incidents, providing "*a structured approach to preparing for, detecting, reporting, assessing, and responding to incidents, and applying lessons learned*".[144] It also adds that every company or organization that wishes to have a strong information security system must follow this designed scheme.

While there are other certifications, these standards are a good example of good practices that help companies and organizations comply with the requirements of the GPDR.

4.1.3. Implementing a security incident response plan

Along with the help of the controls established by ISO/IEC 27035, for example, a well-structured security incident response plan is fundamental for efficiently handling information security incidents. This plan should outline a clear and methodical approach to handling personal data breaches, beginning with planning and preparation to ensure that the company or organization in question is equipped to respond effectively. The next phase involves detection and assessment, where potential breaches are identified and their severity is evaluated. Once a breach is confirmed, the organization must initiate notification and communication procedures, ensuring that SA's and affected data subjects are informed within the timeframes stipulated by the GDPR.

Following a personal data breach, companies and organizations can follow a two-stage impact assessment as outlined by the NIS 2 Directive, as previously studied. First, an initial assessment within 24 hours of detection to determine the cause, nature and severity of the incident. Then, a detailed assessment within 48 hours to evaluate the impact on the business and individuals.

Companies and organizations must do proper investigation and documentation of security incidents and personal data breaches, as a legal and operational necessity. By maintaining well-documented records, companies and organizations can demonstrate their commitment to regulatory compliance and to continuously improve their security practices. A structured review and improvement process should be in place in order to analyze past incidents and refine security strategies accordingly.[145]

Besides the implementation of a security incident response plan, and to further protect personal data, organizations must also adopt technical and organizational security measures, as

[144] ISO/IEC 27035-1:2023 – *Information technology – Information security incident management – Part 1: Principles and process*

[145] Julakanti, S. R., Kiranmayee Sattiraju, N. S., & Julakanti, R. (2025). Data Protection through Governance Frameworks. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2502.10404

outlined by Article 32 of the GDPR. Some of these measures are data minimization, pseudonymization, encryption, access control mechanisms and physical security measures.

4.1.4. Promoting training, awareness, and resource investment

For the present dissertation, we had the opportunity to interview a Cybersecurity Officer, who mentioned the importance of training people and investing in cybersecurity. The officer suggested that regular training and awareness programs are essential for ensuring that employees understand information security and their responsibilities regarding data protection. Training should be tailored to different roles within the organization, emphasizing best practices for data handling, breach reporting, and maintaining strong security practices. Continuous education helps reduce human errors that could lead to breaches and ensures a proactive approach to data protection. It also fosters a culture of transparency, and reduces the stigma around personal data breaches. By normalizing discussions about security incidents and personal data breaches, stakeholders are more likely to trust the organization's commitment to data protection.[146]

Alongside training, investing in human and material resources is crucial for building a resilient security infrastructure. Companies must allocate sufficient resources for preventive security measures, incident response teams, and ongoing risk assessments. A well-funded security strategy reduces the likelihood of personal data breaches and ensures that when security incidents do occur, they are handled efficiently.

[146] Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M. A., Hartley, L., & Lewinsmith, W. (2021). Evaluation of security training and awareness Programs: Review of current practices and guideline. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2112.06356

Conclusion

The GDPR stands as a monumental achievement in the realm of data protection, setting a global benchmark for privacy and security. However, it is important to recognize that the GDPR is not the first legislative attempt to regulate personal data and privacy. Previous laws, such as the Data Protection Directive and the ePrivacy Directive, provided foundational frameworks for data protection,[147] but the GDPR takes these concepts much further, establishing more stringent and comprehensive rules. The GDPR has notably shifted the regulatory landscape by granting individuals greater control over their personal data, enhancing their rights to access, rectification, and erasure of data. This regulatory evolution reflects the increasing recognition of personal data as a key asset that requires robust safeguards to prevent misuse.[148] Yet, despite its strengths, the GDPR's implementation and the broader landscape of data protection face significant challenges.

The increasing frequency of personal data breaches remains one of the most pressing concerns under the GDPR. Personal data breaches have become a near-constant feature in today's digital landscape, where cyber threats are evolving in sophistication and scale. While the GDPR requires organizations to notify DPA's within 72 hours after becoming aware of a personal data breach, the reality is that these incidents are on the rise and many go unreported. Various factors contribute to this underreporting, with one of the most significant being the fear of reputational damage. Organizations are often reluctant to disclose breaches due to concerns that doing so may damage their public image and stakeholders trust. Additionally, there are administrative costs and potential legal consequences that organizations may wish to avoid by delaying or forgoing notifying altogether.[149]

As previously mentioned, Article 33 of the GDPR introduces a critical requirement for controllers to notify DPA's of a personal data breach within 72 hours of becoming aware of it. This 72-hour timeframe is designed to ensure prompt action, but it is often criticized for being unrealistic, especially in the face of increasingly complex and sophisticated cyber threats. Detecting and assessing a personal data breach's full scope within such a narrow window is a monumental challenge for many companies and organizations. Security incidents often involve a multifaceted investigation, requiring time to analyze whether personal data was actually

[147] Wong, R. (2013). Data security breaches and privacy in Europe. In *SpringerBriefs in cybersecurity*. https://doi.org/10.1007/978-1-4471-5586-7

[148] Wolford, B. (2023). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

[149] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026.

compromised and to determine the extent of the damage. For smaller organizations, especially those without dedicated data protection teams or resources, adhering to this deadline can be even more difficult.

The limitations of the 72-hour notification window become more evident when compared to other frameworks, such as the NIS 2 Directive. The NIS 2 Directive adopts a two-step notification process, requiring an initial notification within 24 hours, followed by a more detailed report within 72 hours. This approach recognizes the need for flexibility, ensuring that initial responses can be made quickly, while still allowing time for thorough investigation and analysis. By adopting such a model, the GDPR could better account for the complexities involved in identifying, assessing, and notifying personal data breaches in a timely manner.

A further complication in ensuring comprehensive protection and timely reporting lies in the discrepancy between the legal definitions of a 'personal data breaches' and 'security incident'. The GDPR defines personal data breaches in a narrow sense, focusing primarily on breaches of security where personal data is exposed, lost, or altered in an unauthorized manner. However, not all security incidents necessarily result in a compromise of personal data, yet they could still pose significant risks to individuals' privacy and security. The failure to capture this broader spectrum of security incidents in the GDPR can lead to critical gaps in regulatory coverage. As the nature of cyber threats evolves, the need for a more flexible and expansive understanding of breaches becomes increasingly important.[150]

Another challenge under the GDPR lies in the conflicting motivations of controllers when it comes to personal data breach notifications. The GDPR may create an environment where controllers must balance their legal obligations to report breaches with the potential costs of doing so. High fines and reputational damage can deter organizations from reporting personal data breaches, particularly when they are unsure of whether the incident constitutes a personal data breach as defined by the regulation. Moreover, sanctions for non-compliance may have the unintended consequence of over-deterrence, leading some companies to report incidents that do not rise to the level of a personal data breach, simply to avoid penalties.[151]

The fear of legal consequences and reputational damage may even incentivize some organizations to avoid discovering personal data breaches altogether, in order to evade the obligation to notify. This under-deterrence of personal data breaches erodes the intent of the

[150] Alunge, R. (2020). *Breach of security vs personal data breach: effect on EU data subject notification requirements*. International Data Privacy Law, 11(2), 163-181. https://doi.org/10.1093/idpl/ipaa021.
[151] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026.

GDPR, which seeks to promote a culture of transparency and accountability.[152] Therefore, while the regulation is robust, the current approach may inadvertently encourage behaviors that undermine the effectiveness of the GDPR.

Given the complex landscape of data protection and security, several recommendations can be made to improve the effectiveness of the GDPR. First, companies should establish comprehensive, tailored data protection policies that align with the specific risks and needs of their activities. A one-size-fits-all approach is inadequate in the face of the diverse nature of cyber threats, and a more personalized approach would ensure that organizations can effectively respond to data protection challenges.

Second, the use of codes of conduct and certification mechanisms can help standardize data protection measures, providing clear guidelines for organizations to follow and offering a means for companies to demonstrate their compliance with the GDPR. These tools can improve the consistency and reliability of data protection practices.

Another important recommendation is the development of an effective incident response plan. This plan should outline a clear, methodical approach to identifying, assessing, and reporting personal data breaches.

The GDPR needs to adopt a more flexible approach to personal data breach notification. A two-tiered notification system, as implemented by the NIS 2 Directive, could offer more realistic timelines for reporting personal data breaches. This approach would allow organizations to make a faster initial notification, while still ensuring that detailed reports are provided within a reasonable time, giving them the necessary flexibility to full assess and respond to incidents, and that the concerned data subjects can take the necessary protective measures. This would also guarantee the harmonization of the EU data protection framework with the EU information security framework, as they are intertwined.

At last, but not least, by investing in training and awareness programs for employees, organizations can ensure that everyone within the organization understand their roles and responsibilities in protecting personal data and responding to security incidents.[153]

The GDPR has undeniably raised the global standard for data protection and privacy, providing individuals with essential rights and a sense of control over their personal data. However, to remain effective in an increasingly complex cyber landscape, the regulation must evolve alongside the growing sophistication of threats. A more flexible, proactive approach,

[152] Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, 34(6), 1232-1246. https://doi.org/10.1016/j.clsr.2018.05.026.
[153] Testimony from a Cybersecurity Officer, interviewed for the purpose of writing this dissertation.

supported by better-defined legal frameworks, tailored organizational policies, advocacy of awareness and transparency attitudes, and enhanced compliance, will ensure that the GDPR continues to protect data subjects effectively in the years to come. As the digital world continues to advance, so too must the regulatory mechanisms that safeguard it.

BIBLIOGRAPHIC REFERENCES

Doctrine

Alunge, R. (2020). Breach of security vs personal data breach: effect on EU data subject notification requirements. *International Data Privacy Law*, 11(2), 163–181. https://doi.org/10.1093/idpl/ipaa021

Bhaimia, S. (2018). The General Data Protection Regulation: the Next Generation of EU Data Protection. *Legal Information Management*, 18(1), 21–28. https://doi.org/10.1017/s1472669618000051

Borgesius, F. Z., Asghari, H., Bangma, N., & Hoepman, J. (2023). The GDPR's Rules on Data Breaches: Analysing their rationales and effects. *SCRIPTed a Journal of Law Technology & Society*, 20(2), 352–382. https://doi.org/10.2218/scrip.20.2.2023.8979

Canto Moniz, G. (2023). *Manual de Introdução à Proteção de Dados*. Almedina.

Chatterjee, C., & Sokol, D. D. (2021). Data security, data breaches, and compliance. In *Cambridge University Press eBooks* (pp. 936–948). https://doi.org/10.1017/9781108759458.064

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review*, 35(6), 105342. https://doi.org/10.1016/j.clsr.2019.105342

Esayas, S. Y. (2015). Breach notification requirements under the European Union Legal Framework: convergence, conflicts and complexity in compliance. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2746834_code2035392.pdf?abstractid=2746834&mirid=1&type=2

Dinger, M. & Wade, J. (2019). "The Strategic Problem of Information Security and Data Breaches" The Coastal Business Journal: Vol. 17, No. 1, Article 1.

Fisher, W., Craft, R. E., Ekstrom, M., Sexton, J., & Sweetnam, J. (2024). *Data Confidentiality: Detect, Respond to, and Recover from Data Breaches.* NIST Special Publication. https://doi.org/10.6028/nist.sp.1800-29

Golla, S. (2017). Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR. *JIPITEC*, 8(1), 70–78. https://www.jipitec.eu/issues/jipitec-8-1-2017/4533/JIPITEC_8_1_2017_Golla.pdf

Hintze, M. (2017). Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency. *International Data Privacy Law*, *8*(1), 86–101. https://doi.org/10.1093/idpl/ipx020

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Jackson, S. (2019). How readable are data breach notifications? *Computer Fraud & Security*, *2019*(5), 6–8. https://doi.org/10.1016/s1361-3723(19)30051-x

Jayatilaka, A., Beu, N., Baetu, I., Zahedi, M., Babar, M. A., Hartley, L., & Lewinsmith, W. (2021). Evaluation of security training and awareness Programs: Review of current practices and guideline. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2112.06356

Julakanti, S. R., Kiranmayee Sattiraju, N. S., & Julakanti, R. (2025). Data Protection through Governance Frameworks. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2502.10404

Karyda, M., & Mitrou, L. (2016). *Data Breach Notification: Issues and Challenges for Security Management*. AIS Electronic Library (AISeL). https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1060&context=mcis2016

Kesari, A. (2022). Do data breach notification laws work? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4164674

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, 135, 559-571. https://doi.org/10.1016/j.jbusres.2021.06.054

Lambrinoudakis, C. (2018). The General Data Protection Regulation (GDPR) ERA: Ten Steps for Compliance of Data Processors and Data Controllers. In *Lecture notes in computer science* (pp. 3–8). https://doi.org/10.1007/978-3-319-98385-1_1

Mantelero, A., Vaciago, G., Esposito, M. S., & Monte, N. (2020). The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, *28*(4), 297–328. https://doi.org/10.1093/ijlit/eaaa021

Nahai, F. (2018). General Data Protection Regulation (GDPR) and data Breaches: what you should know. *Aesthetic Surgery Journal*, *39*(2), 238–240. https://doi.org/10.1093/asj/sjy296

Nieuwesteeg, B., & Faure, M. (2018). An analysis of the effectiveness of the EU data breach notification obligation. *Computer Law & Security Review*, *34*(6), 1232–1246. https://doi.org/10.1016/j.clsr.2018.05.026

O'Brien, R. (2016). Privacy and security. *Business Information Review*, *33*(2), 81–84. https://doi.org/10.1177/0266382116650297

Pereira da Silva, J. (2024). *Direitos Fundamentais para o Universo Digital*. Fundação Francisco Manuel dos Santos.

Pereira da Silva, J. (2020). *RGPD: ensaio sobre o novo habitat do direito fundamental à proteção de dados pessoais*. Universidade Católica Editora.

Porcedda, M. G. (2018). Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer Law & Security Review*, *34*(5), 1077–1098. https://doi.org/10.1016/j.clsr.2018.04.009

Sharma, N., Oriaku, E. A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33–41. https://doi.org/10.20448/2001.81.33.41

Shastri, S., Wasserman, M., & Chidambaram, V. (2019). *The Seven Sins of Personal-Data Processing Systems under GDPR*. arXiv.org. https://arxiv.org/pdf/1903.09305.pdf

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9, 11895-11910. https://doi.org/10.1109/access.2021.3051633

Wong, R. (2013). Data security breaches and privacy in Europe. In *SpringerBriefs in cybersecurity*. https://doi.org/10.1007/978-1-4471-5586-7

Legislation

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

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 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).

Directive 95/46/EC (Data Protection Directive) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EU Charter of Fundamental Rights

European Convention on Human Rights

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection natural persons with regard to the processing of personal data and on the free movement of such data.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

Universal Declaration of Human Rights

Guidelines

Commission Nationale Informatique & Libertés. *GPDR developer's guide*. https://www.cnil.fr/en/gdpr-developers-guide

Commission Nationale Informatique & Libertés. *Security of Personal Data*. Version 2024.

European Network and Information Security Agency. *Recommendations for a methodology of the assessment of severity of personal data breaches*. December 2013.

European Data Protection Board. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification.* Version 2.0. Adopted 14 December 2021.

European Data Protection Board. *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*. Version 2.1. Adopted 24 May 2023.

European Data Protection Board. *Guidelines 9/2022 on personal data breach notification under GDPR*. Version 2.0. Adopted 28 March 2023.

European Data Protection Board. *Guidelines on personal data breach notification for the European Union Institutions and Bodies*. Adopted 7 December 2018.

European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law*. 2018 edition.

Article 29 Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Adopted 4 October 2017.

Standards

ISO/IEC 27001:2023 – *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

ISO/IEC 27002:2022 – *Information security, cybersecurity and privacy protection – Information security controls*

ISO/IEC 27035-1:2023 – *Information technology – Information security incident management – Part 1: Principles and process*

Case law

Decision Under S.111 of the Data Protection Act 2018 and for the Purposes of Article 60 of the General Data Protection Regulation (EU) 2016/679 (GDPR). DPC Case Reference: IN-19-1-1.

Decision of the AP against Booking.com, from 10 December 2020.

Decision of the UODO against Santander Bank Polska, from 12 March 2024. Case Reference: DKN.5131.59.2022

Decision of the UODO against Santander Bank Polska, from 19 January 2022. Case Reference: DKN.5131.33.2021

Others

Council of Europe. *Convention 108 and Protocols*. https://www.coe.int/en/web/data-protection/convention108-and-protocol

Data Protection Commission. (2023). *Annual Report from 2023*. https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2023-annual-report

European Commission. *Data protection explained*. https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

European Commission. *Legal framework of EU data protection*. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

European Commission. *What is a data breach and what do we have to do in case of a data breach?* https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en

European Council. *The general data protection regulation*. https://www.consilium.europa.eu/en/policies/data-protection-regulation/

European Data Protection Board. Annual Report 2023.

European Data Protection Board. *Guidelines*. https://www.edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en

European Data Protection Supervisor. (2023) *Personal Data Breach*. https://edps.europa.eu/data-protection/our-role-supervisor/personal-data-breach_en

IBM. *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

IBM. *What is Data Exfiltration?* https://www.ibm.com/think/topics/data-exfiltration

IBM. *What is Cybersecurity?* https://www.ibm.com/topics/cybersecurity

GDPR Enforcement Tracker. https://www.enforcementtracker.com

GDPRhub. https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub

NIST Glossary. *Cyber Threat*. https://csrc.nist.gov/glossary/term/cyber_threat

NIST. Small Business Cyber Corner. Ransomware. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

Wolford, B. (2022). What is GDPR, the EU's new data protection law? *GDPR.eu*. https://gdpr.eu/what-is-gdpr/

Wolford, B. (2023). *Does the GDPR apply to companies outside of the EU?* GDPR.eu. https://gdpr.eu/companies-outside-of-europe/

Wolford, B. (2023). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/