The Data Breach Notification

Obligation in the GDPR

Assessing the Interpretative and Practical Problems Posed by the Obligation

Selle, Oda Josefine Borke

Candidate number: 8012
Submission deadline: 01.12.2020
Number of words: 17 619
Table of contents

1  INTRODUCTION ........................................................................................................... 1
   1.1 The General Data Protection Regulation (GDPR) and the Data Breach Notification
       Obligation .................................................................................................................. 1
   1.2 Relevance of Research ............................................................................................ 2
   1.3 Research Question ................................................................................................. 3
   1.4 Research Methodology ........................................................................................... 4
   1.5 Structure ................................................................................................................ 5

2  BACKGROUND ............................................................................................................ 6
   2.1 The GDPR and Security ........................................................................................ 6
   2.1.1 Risk-Based Regulation and the GDPR ............................................................... 7
   2.2 The DPD and the GDPR ....................................................................................... 8
   2.3 An Introduction of Selected Provisions in the GDPR .......................................... 9
   2.4 The Development of the Data Breach Notification Obligation ............................... 10
   2.5 Data Breach Notification Obligations in the EU Legal Framework ....................... 12
   2.6 Summary .............................................................................................................. 13

3  SECURITY IN THE GDPR ...................................................................................... 13
   3.1 Overview .............................................................................................................. 13
   3.2 Legislative Analysis of the GDPR ........................................................................ 14
   3.2.1 Personal Data, Processing and Controllers & Processors ................................ 14
   3.2.2 Article 3 – Territorial Scope ........................................................................... 15
   3.2.3 Articles 30 & 35 – Records of Processing Activities and Data Protection
       Impact Assessment .................................................................................................. 16
   3.2.4 Data Protection Authorities ............................................................................. 16
   3.2.5 Article 32 – Security of Processing .................................................................. 17
   3.2.6 Article 34 – Communication of a Personal Data Breach to the Data Subject .. 18
   3.2.7 Article 83 – General Conditions for Imposing Administrative Fines ............. 19
   3.3 The Intricacies of the Security Provisions Throughout the GDPR ..................... 19
   3.4 Critical Analysis of the GDPR ............................................................................ 22
   3.4.1 Harmonisation of the European Data Protection Sphere............................... 22
   3.4.2 Rights of Data Subjects and Transparency ..................................................... 23
   3.4.3 Article 32 - Security .................................................................................... 24
   3.4.4 Article 34 – Data breach Notification to Data Subjects .................................. 26
   3.4.5 The Notion of Risk and High Risk in Articles 33 and 34 ............................... 27
3.4.6  Article 83 - Fines ........................................................................................................... 28
3.5  Security in the Data Protection Context ........................................................................ 29
3.6  Summary ........................................................................................................................ 32

4  THE DATA BREACH NOTIFICATION OBLIGATION IN THE GDPR ........... 32
4.1  Overview ......................................................................................................................... 32
4.2  Legislative Analysis of Article 33 - Notification of a Personal Data Breach to the
    Supervisory Authority – and Interpretative Problems ..................................................... 33
4.3  Practical Difficulties Related to the Data Breach Notification in the GDPR .............. 35
4.4  Purposely Withholding Notification of an Ongoing Data Breach as a Mitigation
    Measure ............................................................................................................................. 36
4.5  Over-Notification of Data Breached to DPAs and Notification Fatigue .................. 36
4.6  Analysing Risks to the Rights and Freedoms of Data Subjects ................................. 38
4.7  Purposely not Detecting Data Breaches ...................................................................... 38
4.8  Data Breach Notification and the Lack of Security ..................................................... 39
4.9  Small and Medium- Sized Enterprises and the Data Breach Notification Obligation... 40
4.10  Personal Data Breaches: Reputational Damage or a Competitive Advantage? ......... 40
4.11  The Role of the Data Protection Authorities ................................................................. 41
4.12  The Issue of Multiple Data Breach Notification Obligations in EU Law .................. 42
4.13  Summary ........................................................................................................................ 43

5  CONCLUSION ....................................................................................................................... 44

TABLE OF REFERENCE ........................................................................................................... 46
EU Legislative Instruments ........................................................................................................ 46
EU Documents ........................................................................................................................ 46
Books and Chapters .................................................................................................................. 47
Journal Articles ........................................................................................................................ 48
Other Sources .......................................................................................................................... 50
1 Introduction

Data breaches are a daily occurrence worldwide, constituting a major risk to the future of global business.\(^1\) With a global average price of $3.86 million USD,\(^2\) a single data breach notification represents a fundamental challenge for entities operating in today’s digital society. Aside from the financial implications which may follow a data breach, the affected entity might also incur reputational damage, as well as technical and organisational challenges. Additionally, where the data compromised is personal data, it could also have detrimental consequences for the individuals affected. As such, the European Union (EU), through the General Data Protection Regulation (GDPR),\(^3\) imposes a data breach notification obligation on controllers and processors of personal data,\(^4\) as well as an overall security requirement,\(^5\) to tackle the issue personal data breaches.

1.1 The General Data Protection Regulation (GDPR) and the Data Breach Notification Obligation

Two of the main instruments the EU employs when regulating are Regulations and Directives. A Regulation is legally binding and is directly applicable and enforceable in all Member States of the EU.\(^6\) A Directive is also legally binding, yet there are allowances for how the Member States approach the implementation of the Directive into national law.\(^7\) As a point of context, it is important to briefly introduce the GDPR and what a data breach notification is.

The GDPR is arguably a global standard-setter in the field of data protection,\(^8\) regulating the processing and the free movement of personal data.\(^9\) The Regulation is extensive, with 173

---


\(^3\) EU, Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), Regulation 2016/679.

\(^4\) Ibid. (GDPR), Article 33.

\(^5\) Ibid. (GDPR), Article 32.


\(^7\) Ibid. (Craig & De Bürca), p. 138-139.

\(^8\) EU Commission, Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation, COM (2020) 264 final, p. 3.

\(^9\) GDPR, Supra note 3, Article 1.
Recitals and 99 Articles dealing with various aspects falling within the scope of data protection. As a point of clarification, recitals in EU law set out the reasons behind the provisions in the Regulation and are not legally binding *per se*.

Generally, note the GDPR it is a fairly comprehensive legislation and navigating the numerous provisions may be difficult.

In the GDPR, a data breach notification is the act of notifying the relevant Data Protection Authority (DPA), and possibly the affected data subjects, where there is a risk or a high risk to the rights and freedoms of data subjects, arising from a data breach. To further clarify, a data subject is any identified or identifiable natural person to whom the data relates. By notifying the relevant authority or data subjects, the entity victim of a data breach might be able to mitigate the effects of the breach, thereby also potentially mitigating organisational and financial losses. As a further benefit, the notifying entity might also receive appropriate guidance from the DPA as to how to deal with the breach.

### 1.2 Relevance of Research

The GDPR is a topical subject, especially as it is now over two years since it became enforceable. This may arguably come down to the fact that the GDPR is considered to set a high global standard of data protection, coupled with the possibility of imposing substantial financial repercussions for non-compliance with the Regulation. Consequently, the number of related publications has increased, and the focus has shifted from theory to application. It is interesting to note that, compared to other aspects set forth by the GDPR, such as consent or the ‘right to be forgotten’, the data breach notification obligation has not enjoyed the same level of research. It is often addressed as an element in a broader discussion on the GDPR, but it is rarely dealt with on its own and analysed in a broader security context. Interestingly, data
breaches enjoy wide interest in the media, something which is not necessarily reflected in academia.

Initially, it is important to address why there is a need to have a data breach notification obligation. The possible consequences of data breaches are vast, and historically, in the minds of the entities affected by a data breach, it is often considered to be in the entity’s best interest to keep information about a data breach under lock and key. Considering the intricacies of the digital economy, processing of personal data can be highly lucrative, and such entities should be held accountable for security breaches concerning personal data resulting in a risk to data subjects. As such, as a step to aid in the safeguarding of the rights and freedoms of data subjects, there is a clear need for a mandatory notification obligation like the one found in the GDPR, which requires the notification be made to a DPA. This facilitates entity accountability under the Regulation.\footnote{Ibid. (GDPR), Article 5 (2).} As such, the data breach notification obligation is an essential element of security in the GDPR, seeing as a breach will often shed light on whether or not the GDPR has been complied with.\footnote{Burton, “Article 32. Security of Processing” in Kuner, Bygrave & Docksey (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press (2020), p. 632.}

Seeing as the GDPR is a key legislative instrument in the field of data protection, in conjunction with the possible detrimental effects arising from a data breach, it is of high relevance to conduct further analysis on the problems caused by the data breach notification obligation and its risk-based approach.

### 1.3 Research Question

With an emphasis on the importance of a data breach notification obligation in the realm of data protection, the research question is thus: what are the interpretative and practical problems posed by the data breach notification obligation in the GDPR? The question is phrased so that it will holistically examine the data breach notification obligation in Article 33 of the GDPR, with the GDPR and its security requirement as its fundamental basis. To answer the research question, a series of sub-questions are raised. What is a risk-based approach in the GDPR? Which provisions in the GDPR are intimately related to the data breach notification
obligation and the security obligations? How does the overall security focus of the GDPR tie into the data breach notification obligation?

The basic argument of this thesis is that the data breach notification obligation does not necessarily provide a more practical approach to regulation for entities processing personal data. This is based on the analysis of the factors tied to the data breach notification obligation, with an emphasis on problems relating to the interpretation of the obligation itself, the practical application of the obligation, the diffuse nature of the phrasing used in the relevant Article in the GDPR, the lack of a definition of risk in the Regulation, as well as incentives to adhere to the data breach notification obligation, reducing the practicality of the obligation. For the obligation to be more practically sensible, there needs to be further elaborations from relevant EU authorities, further delineating and defining certain aspects of the obligation, as well as addressing how to deal with the problems tied to the obligation raised in this thesis.

1.4 Research Methodology

This thesis utilises desk research as its main research methodology. It assesses the legislative framework in the field of data protection in the EU, scholarly work such as journal Articles and books, as well as guidelines, reports and media coverage, analysing the data breach notification obligation and the security provisions in the GDPR. As a point to note, bodies such as the European Data Protection Board (EDPB)19 are tasked with issuing opinions of a non-binding character which will be utilised in this thesis. They are seen as essential to clarify issues in the realm of data protection.20 However, it does not mean that EDPB’s opinions are infallible or are to be taken at face value. As with all the sources utilised, it is vital to keep a critical perspective when assessing their opinions and to analyse them in an unbiased manner. It would furthermore be natural to address the guidance provided by the Court of Justice of the EU (CJEU) within the area of data breach notification, seeing as the court issues legally binding decisions often clarifying principles of EU law. However, the CJEU has not dealt

19 Formerly the Article 29 Working Party.
with any cases concerning the data breach notification obligation specifically,\textsuperscript{21} which means that this thesis will only be using the general interpretive approach of the CJEU in analysing the GDPR. By utilising the aforementioned sources, critical thinking and in-depth legal analysis, this thesis analyses the GDPR as a data protection instrument with an overall security focus, before analysing the data breach notification and its problems.

1.5 Structure

This thesis is split into three main chapters, where chapter 2 provides relevant background information, chapter 3 deals with security in the GDPR and chapter 4 tackles the issues posed by the data breach notification obligation.

Chapter 2 of this thesis provides some relevant background information and analysis concerning the Regulation and its regulatory approach. This creates a baseline of knowledge enabling the assessment of the data breach notification obligation in the context of the security provision in the GDPR. It also looks at the evolution from the 1995 Data Protection Directive\textsuperscript{22} to the GDPR. Furthermore, it addresses the origins of the data breach notification obligation, as well as the EU’s approach to data breaches in legislative instruments outside of the GDPR.

Considering the possible adverse consequences for data subjects following a personal data breach and other security incidents, coupled with the possible repercussions for the entity processing the personal data, chapter 3 closely analyses the GDPR (with the exception of Article 33 which is analysed in chapter 4), as it can be argued to be a vital instrument in ensuring adequate protection for data subjects. This analysis looks at the GDPR, its relevant Recitals and Articles related to security, and sets out other relevant provisions concerning processing, controllers and processors, DPAs and fines. It then provides a roadmap analysing security in the provisions of the GDPR, before it deals with criticism in relation to the provisions of the Regulation dealt with in the chapter. Following this analysis, the thesis conducts a broader analysis of the impact of security within the field of data protection, with reference to the GDPR.


\textsuperscript{22} EU, Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Directive 95/46/EC.
Finally, chapter 4 focuses on the data breach notification obligation, setting out the legislative provision in the GDPR, as well as a critique of it. Furthermore, the chapter analyses the problems related to the data breach notification obligation, including the practical difficulties of performing a notification, withholding a notification to be able to implement mitigation measures, over-notification of low-risk data breaches, detection of data breaches, key issues related to small and medium sized enterprises, the role of the supervisory authorities and the issue of multiple breach notification obligations in the EU, before concluding.

2 Background

2.1 The GDPR and Security

The EU has a solid foundation for which it can legislate within the area of data protection. With the adoption and subsequent entering into force of the GDPR, the EU has been hailed as the “world’s privacy cop”. This is based on the fact that the GDPR extends well beyond its borders, enabling it to have a significant impact as a standard-setting instrument in the area of privacy and data protection. The GDPR regulates the processing and free movement of personal data, but as a point to note, it does not legislate in every area within the data protection sphere.

As a point of clarification, it is important to note that security does not automatically equate to data protection afforded to the data subjects. The aims of data security can just as easily be to protect the interests of controllers and processors, just as much as to protect the rights and freedoms of data subjects. This thesis appreciates the possible contradictory aims of security, clarifying that security in this context concerns data security in line with the GDPR’s aim to protect the rights and freedoms of data subjects.

25 Based on its territorial scope; see GDPR, Supra note 3, Article 3.
26 EU Commission, Supra note 8, p. 3.
27 GDPR, Supra note 3, Article 1.
30 Ibid. (Bygrave), p. 2.
2.1.1 Risk-Based Regulation and the GDPR

Before tackling some of the relevant provisions and aspects of the GDPR and the development from the Data Protection Directive to the GDPR, it is relevant to address the GDPR’s regulatory risk-based approach to data protection. This approach complements the more familiar rights-based approach often taken in EU legislation. The move towards a risk-based regulatory approach within data protection has been spurred on by technological development and its ensuing challenges, making the traditional methods of regulation based on an elaboration of core data protection principles fall short as the sole method for regulation.31 This risk-based granulated approach is arguably better able to meet the challenges posed by technological development and data protection,32 as it centres around assessing the risks tied to the processing activity, making it the decisional basis of whether or not to go forward with the proposed processing.33 One of the benefits of a risk-based approach is the ability to individually determine the risks posed to the processing activity at hand, and implement the appropriate safeguards and mitigating factors in each case.34 This arguably provides a more practical approach to data protection.35

Yet a purely risk-based approach can also be argued to go against the aim of the Regulation within the data protection sphere. This criticism centres around the fact that its protection might be uneven in terms of determining the risks posed, which may contravene the level of protection afforded to data subjects.36 The risk-based approach in the GDPR is therefore limited to the compliance with the obligations set out in the Regulation, such as the data processing impact assessment37 and the data breach notification obligation.38 Ergo, the Regulation enjoys a firm rights-based approach, as the core-principles outlined are still rights-

32 Ibid. (Gellert), p. 483.
33 Ibid. (Gellert), p. 482.
34 Ibid. (Gellert), p. 490.
36 Gellert, Supra note 31, p. 483.
37 GDPR, Supra note 3, Article 35.
38 Ibid. (GDPR), Article 33; Gellert, Supra note 31, p. 483.
based\textsuperscript{39}, operating in tandem with the added risk-based approach introduced in its data protection obligations.

2.2 The DPD and the GDPR

The DPD\textsuperscript{40} provided a solid foundation for data protection in the EU. When it came into force, it was considered the “most ambitious, comprehensive and complex”\textsuperscript{41} within the area of data protection. However, the DPD failed in one of its fundamental aims; to sufficiently harmonise the various data protection legislations across EU Member States.\textsuperscript{42} Seeing as the legislative instrument chosen was a Directive, the Member States enjoyed a large degree of freedom in how its provisions would be implemented in their national laws.\textsuperscript{43} This resulted in a lack of harmonisation under the Directive, which in turn caused legal uncertainty in the area of data protection.\textsuperscript{44} This uncertainty was perceived to be a challenge to the economic activities within the EU,\textsuperscript{45} as processing activities that were considered to be legal in one Member State may not have been permitted in another Member State.\textsuperscript{46} There was therefore a need to further develop, enhance, and harmonise the European efforts within the data protection sphere, which was met through the enactment of the GDPR.

As the GDPR is a Regulation, Member States enjoy less freedom in its implementation, ensuring an equivalent level of protection across the EU.\textsuperscript{47} The differences between the DPD and the GDPR were not solely the choice of legislative instrument; the GDPR has developed and added a series of data protection principles, obligations and rights, expanding the protection of rights and freedom of data subjects, and further developing the area of data protection in the EU. A selection of the developments made in the GDPR are the introductions of the data breach notification obligation,\textsuperscript{48} the principle of data protection by design and by de-

\textsuperscript{39} Ibid. (Gellert), p. 483.
\textsuperscript{40} DPD, Supra note 22.
\textsuperscript{41} Bygrave, Supra note 29, p. 53.
\textsuperscript{42} GDPR, Supra note 3, Recital 9; Voigt & Von dem Bussche, Supra note 28, p. 1.
\textsuperscript{43} Craig & De Búrca, Supra note 6, p. 138-139.
\textsuperscript{45} GDPR, Supra note 3, Recital 9.
\textsuperscript{46} Voigt & von dem Bussche, Supra note 28, at p. 2.
\textsuperscript{47} GDPR, Supra note 3, Recital 10.
\textsuperscript{48} Ibid. (GDPR), Article 33.
fault,\textsuperscript{49} the right to erasure,\textsuperscript{50} the right to data portability,\textsuperscript{51} and the introduction of the principle of accountability as a principle in its own right,\textsuperscript{52} as well as the amplification of the possible fines incurred by non-compliance.\textsuperscript{53} The GDPR therefore imposes a series of new obligations on controllers and processors as opposed to the DPD.\textsuperscript{54}

In the context of security and the data breach notification obligation, Article 17 of the DPD set out the previously applicable security provision. Article 32 of the GDPR mimics to a certain extent the security rationale contained in DPD Article 17. The main difference between the two is that the GDPR is explicitly applicable to controllers and processors alike, whilst the DPD requirement was explicitly applicable to controllers, and only implicitly applicable to processors.\textsuperscript{55} Additionally, where the DPD set out the need to prevent data breaches, it did not contain a separate data breach notification obligation.\textsuperscript{56} The GDPR therefore goes further than the DPD by adding the two separate data breach notification obligations,\textsuperscript{57} and making the security requirement expressly applicable to all relevant entities processing personal data.

\subsection*{2.3 An Introduction of Selected Provisions in the GDPR}

As a point of departure, it is relevant to assess the definition of personal data in the GDPR, seeing as processing of personal data is at the core of the Regulation. The definition of personal data can be viewed as expansive as it covers a wide array of identifiers, concerning both identified and identifiable natural persons.\textsuperscript{58} This enables a broad scope of application when it comes to the GDPR. As most information can be considered personal data under this definition, it arguably enhances the protection and control of data subjects and strengthens their rights.\textsuperscript{59}

\begin{thebibliography}{99}
\bibitem{49} Ibid. (GDPR), Article 25.
\bibitem{50} Ibid. (GDPR), Article 17.
\bibitem{51} Ibid. (GDPR), Article 20.
\bibitem{52} Ibid. (GDPR), Article 5 (2).
\bibitem{53} Ibid. (GDPR), Article 83; Voigt \& von dem Bussche, \textit{Supra} note 28, at p. 2.
\bibitem{54} Bygrave, \textit{Supra} note 29, p. 186.
\bibitem{55} Burton, \textit{Supra} note 18, p. 632.
\bibitem{56} Burton, \textit{Supra} note 21, p. 642.
\bibitem{57} GDPR, \textit{Supra} note 3, Articles 33 \& 34.
\bibitem{58} Ibid. (GDPR), Article 4.
The GDPR also has a strong security focus when it comes to regulating the processing of personal data. In fact, this is one of the basic principles of the Regulation. Chapter IV, Section 2 of the Regulation builds on this principle and sets out obligations relating to the security of processing of personal data, notification of a personal data breach and communication of a personal data breach to the data subject. Combined, these provisions aim to ensure an adequate level of security, both on the technical and organisational level, potentially mitigating consequences of data breaches, as well as ensuring compliance with the Regulation. The security focus of the GDPR places responsibility on affected entities to take appropriate steps to prepare for and, to a certain extent, mitigate the negative consequences resulting from a data breach. When assessed in the context of the broad definition of personal data in the GDPR, it is clear these security provisions have a wide scope of application and are essential in safeguarding the rights and freedoms of data subjects.

2.4 The Development of the Data Breach Notification Obligation

Before dealing with the legislative analysis of the GDPR, it is relevant to set out what a data breach is defined as in the Regulation, where it originated, as well as setting out the different breach notification obligations in the EU. The GDPR defines a data breach as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. As outlined in the introduction, the consequences of a data breach can be immense, including financial, organisational and reputational aspects, underlining the need for a mandatory data breach notification obligation.

The first data breach notification legislation was enacted in California, in 2003. This is interesting, as the U.S. is not necessarily the first country that comes to mind when discussing

61 GDPR, Supra note 3, Article 32.
62 Ibid. (GDPR), Article 33.
63 Ibid. (GDPR), Article 34.
65 GDPR, Supra note 3, Article 4 (12).
66 California Civil Code, Sections 1789.29 and 1789.82.
issues related to the protection of the rights and freedoms of data subjects, and the secure processing of personal data. It is also intriguing to note that arguably, the data breach notification obligation in the GDPR takes inspiration from the California legislation. The notification law passed in California was a positive development in the area of privacy and data protection in the U.S., spurring enactment of several similar laws in other states, leading to increased protection for data subjects in the U.S. As a matter of fact, as of January 2020, all 50 states in the U.S. have passed legislation pertaining to data breach notifications. Yet this myriad of state laws concerning data breaches has created a difficult landscape of notification laws for entities to navigate. Combined with federal laws that are industry-specific, for areas such as health-care, financial institutions and telecoms to name a few, compliance with data breach notification laws in the U.S. poses a significant challenge for entities. Seeing as the data breach notification obligations vary significantly from state to state, a possible way to adequately deal with this complex notification environment could be for entities to adopt internal notification procedures based on where their customers are based, identify which data breach notification legislations are applicable, and tailor the notification procedure to best suit the most stringent data breach notification legislation.

The challenge of different legislative frameworks for data breach notification is not only present in the U.S. The EU also has different legislative instruments dealing with breach notification.

68 Bygrave, Supra note 29, p. 114.
72 DLA Piper, Supra note 70.
2.5 Data Breach Notification Obligations in the EU Legal Framework

As stated in part 2.2, the DPD did not have a mandatory data breach notification obligation. As a consequence, prior to the enactment of the GDPR, some EU Member States had domestic data breach notification requirements, either as hard or soft law instruments. The GDPR has therefore been instrumental in harmonising the different data breach notification legislations within Member States regarding personal data, seeing as Member States enjoy little leeway in how the Regulation is to be implemented in domestic law.

There are also other EU instruments that have a data breach notification obligation, with differing requirements for how to notify. It is relevant to assess these frameworks in tandem with the GDPR to create a roadmap of data breach notification obligations in the EU. The first EU instrument setting out a data breach notification obligation was the e-Privacy Directive from 2002, which concerns electronic communications services. The Directive was an important development in the EU, in that it set a requirement for a higher level of security. Furthermore, there are other EU legislative instruments that have set out a data breach notification obligation; these include the eIDAS Regulation, the NIS Directive, Regulation 611/2013, the PSD2 Directive and the EECC Directive. With a fair number of EU in-
Instruments setting out different data breach notification obligations, it may result in legal uncertainty. This is discussed in part 4.12.

2.6 Summary
This chapter has sought to provide a foundation of the legislative aspects relevant to this thesis, as well as some contextual information. The key takings from this chapter are, firstly, that the EU are leading the way within the area of privacy and data protection with the enactment of the GDPR. Secondly, the GDPR is taking a practical approach to data protection through its risk-based approach, and the Regulation is a welcomed development in the area of data protection building on the foundation of the DPD. Lastly, the notification obligation is not an exclusive EU instrument, and within the EU notification landscape, there are several legal instruments dealing with data breaches.

To assess the problems relating to the data breach notification obligation and the practicality of the risk-based approach taken in the GDPR, this thesis conducts an in-depth analysis of the relevant provisions in the GDPR and provides an overall analysis of its security obligations.

3 Security in the GDPR
3.1 Overview
Data protection and security go hand in hand. As set out in the introduction, entities lacking adequate technical and organisational measures dealing with security might suffer dire economic, reputational and organisational consequences. In today’s digital society, having a comprehensive security focus within a data protection framework is essential. This is based on the fact that we are moving away from whether an entity will suffer a data breach, to when such a breach will occur.87 The following chapter provides a legislative analysis of the GDPR, with the exception of Article 34, which will be covered in chapter 4, a roadmap of the security requirements spanning the GDPR, a critique of selected areas of the Regulation, as well as a broader analysis of the security provisions in the GDPR.

87 Burton, Supra note 18, p. 631.
3.2 Legislative Analysis of the GDPR

Before tackling the Articles dealing with security of personal data in the Regulation, it is relevant to flesh out the short introduction to the GDPR made in chapter 2, before further analysing other relevant Articles. As a recap, the GDPR regulates the processing of personal data, with an emphasis on the protection of data subjects’ rights and freedoms, as well as transfers of data. The Regulation further outlines a series of principles regarding the processing of personal data, with an emphasis on lawfulness, fairness, transparency and accountability.\(^88\) The Regulation underlines that it is technology neutral and is not dependent on the techniques used when it comes to privacy and data protection,\(^89\) which enables a broader scope of application.

What constitutes a risk to the rights and freedoms of data subjects is pertinent, and as such, is referenced throughout this thesis and the GDPR. The Regulation refers to risk as the consequences resulting from the processing of personal data which may incur physical or material/non-material injury to the data subject.\(^90\) It refers to scenarios which, in particular, would constitute a risk, such as identity theft following a personal data breach. In addition to Recital 75, the notion of risk is further developed in Recital 76, where it is stated that risk “should be determined by reference to the nature, scope, context and purpose of the processing”.\(^91\) With reference to the aforementioned Recitals, is it clear the GDPR does give an indication of how to determine risk, in addition to a series of pre-defined risk-scenarios. However, it may be argued that this is too vague, and the notion of risk needs to be expanded in the context of privacy and data protection for it to be fully appreciated. As will be dealt with subsequently, there is no further elaboration of what constitutes risk or high risk to data subjects in the GDPR, which has a significant impact when it comes to data breach notification obligations. This issue is dealt with in parts 3.4.5 and in chapter 4, part 4.6.

3.2.1 Personal Data, Processing and Controllers & Processors

It is relevant to look at what constitutes processing of personal data, as this is one of the main aspects of the Regulation. Article 4 defines processing as operations performed on personal

\(^{88}\) GDPR, Supra note 3, Article 5 (1).

\(^{89}\) Ibid. (GDPR), Recital 15.

\(^{90}\) Ibid. (GDPR), Recital 75.

\(^{91}\) Ibid. (GDPR), Recital 76.
data, enabling a broad scope of application of the GDPR based on this broad definition. In regard the subject matter, as noted in chapter 2, the broad definition of personal data coupled with the possibility of re-identification through reverse-engineering methods substantially widens the reach of the GDPR. The Regulation can therefore be argued to tackle most all cases where there is a processing of personal data.

Furthermore, the Regulation sets out two entities with different obligations under the GDPR when it comes to the processing of personal data: controllers and processors. A controller is an entity which determines the purposes and means of processing, and a processor is an entity which processes data on behalf of a controller. The Regulation sets out six circumstances where the processing of personal data is deemed lawful; where the data subject consents, where such processing is necessary in the performance of a contractual obligation or it is necessary in the pursuance of a legitimate interest by a controller. Conversely, the GDPR sets a higher threshold when it comes to processing of special categories of data, such as data concerning race, religious beliefs, biometric data and health data, to name a few.

3.2.2 Article 3 – Territorial Scope

The GDPR has a broad scope of application, both in terms of territorial reach and subject matter. As for the territorial scope of the Regulation, Article 3 enables the EU to regulate entities established outside the Union within the field of data protection. The Article establishes that entities targeting data subjects in the EU in relation to the provision of goods or services, or

---

92 Ibid. (GDPR), Article 4 (2).
94 De Hert & Papakonstantinou, Supra note 76, p. 180.
95 GDPR, Supra note 3, Article 4 (7); Yet entities are struggling with delineating who is a controller and a processor, which may lead to further issues. However, this is not dealt with in this thesis (Multistakeholder Expert Group to Support the Application of Regulation (EU) 2016/679, Contribution of the Multistakeholder Expert Group to the Commission 2020 Evaluation of the General Data Protection Regulation (GDPR), Report (17 June 2020), p. 23).
96 Ibid. (GDPR), Article 4 (8).
97 Ibid. (GDPR), Article 6 (1) (a).
98 Ibid. (GDPR), Article 6 (1) (b).
99 Ibid. (GDPR), Article 6 (1) (f).
100 Ibid. (GDPR), Article 9.
monitoring their behaviour in the EU, fall within the scope of the Regulation.\textsuperscript{101} Based on this wide territorial reach, coupled with the high standard of protection set out in the Regulation, it is natural that the EU Commission has hailed the EU’s efforts through the GDPR as being a “global standard-setter for the regulation of the digital economy”\textsuperscript{102} in the context of data protection. As data breaches are a global phenomenon, the broad territorial scope of the Regulation is a key feature of the GDPR. As it enables oversight and accountability at a broader level, it is a key instrument within data protection for all data subjects within the EU, as well as outside the Union.

3.2.3 Articles 30 & 35 – Records of Processing Activities and Data Protection Impact Assessment

The GDPR also sets out a requirement to keep records of processing activities.\textsuperscript{103} This includes, where possible, a record of appropriate technical and organisational measures taken to adhere to the security requirement in the Regulation.\textsuperscript{104} These records may play a part in the process of a data breach notification, as the obligation requires that certain information be communicated to the DPAs which may be found in these records of processing. The GDPR also sets out an obligation to conduct a Data Protection Impact Assessment (DPIA) where the processing is likely to result in a high risk to data subjects.\textsuperscript{105} A DPIA may be relevant when assessing whether or not to notify a data breach to data subjects, as the processing activity has already been deemed high risk.\textsuperscript{106} The relevancy of a DPIA when considering the data breach notifications will be further examined later in part 3.4.5.

3.2.4 Data Protection Authorities

Lastly, it is relevant to look at the role afforded to DPAs, as set out in Chapter VI of the GDPR. The role of the DPAs is to monitor the application of the GDPR, as an independent public authority.\textsuperscript{107} The Regulation dedicates a whole Article setting out the notion of DPA independence, underlining the vital role it plays in the protection of the rights and freedoms of

\begin{itemize}
  \item \textsuperscript{101} Ibid. (GDPR), Article 3 (2)(a) & (b).
  \item \textsuperscript{102} EU Commission, Supra note 8, p. 3.
  \item \textsuperscript{103} GDPR, Supra note 3, Article 30.
  \item \textsuperscript{104} Ibid. (GDPR), Article 30 (1) (g) & (2) (d).
  \item \textsuperscript{105} Ibid. (GDPR), Article 35.
  \item \textsuperscript{106} Article 29 Data Protection Working Party, Guidelines on Personal Data Breach Notification Under Regulation 2016/679, 2018/EN WP250rev.01, p. 11-12.
  \item \textsuperscript{107} GDPR, Supra note 3, Article 51 (1).
\end{itemize}
data subjects.\textsuperscript{108} It is important to note that the Regulation stresses the need for adequate “human, technical and financial resources”\textsuperscript{109} in the DPAs to be able to fulfil their duties according to the GDPR, the reality of which will be criticised in chapter 4. Relevant to the discussion at hand, the GDPR defines a set of powers conferred to DPAs. These include, to name a few, investigative powers,\textsuperscript{110} powers to order a ban on processing contrary to the Regulation,\textsuperscript{111} powers to issue reprimands\textsuperscript{112} or warnings,\textsuperscript{113} and importantly, the power to impose fines.\textsuperscript{114} As the gatekeepers of the GDPR, the DPAs therefore play a vital role in the practical application of the Regulation. They are also central to the data breach notification obligation seeing as they are able to impose fines for non-compliance, which will be discussed subsequently.

The above paragraphs have set out the basic legislative provisions needed to get a holistic understanding of the GDPR in the context of this thesis. The following paragraphs will address the security specific Articles within the GDPR, as well as the provision covering financial consequences of non-compliance with the Regulation, as it ties in closely with the security and data breach notification debate.

3.2.5 Article 32 – Security of Processing

Chapter IV of the GDPR sets out the obligations for controllers and processors, and Section 2 of the Chapter concerns security of personal data. The initial Article, Article 32, tackles the issue of security of processing. As a point to note, Article 32 is not the only instance in which the Regulation references security. Such reference is made throughout the GDPR,\textsuperscript{115} and this will be dealt with further in part 3.3. The Article states that controllers and processors need to implement appropriate technical and organisational measures, ensuring an appropriate level of security when considering the relevant risks posed by the processing.\textsuperscript{116} It furthermore provides some leeway to the obligation, seeing as one may take account of the financial aspects

\textsuperscript{108} Ibid. (GDPR), Article 52.
\textsuperscript{109} Ibid. (GDPR), Article 52 (4).
\textsuperscript{110} Ibid. (GDPR), Article 58 (1).
\textsuperscript{111} Ibid. (GDPR), Article 58 (2) (f).
\textsuperscript{112} Ibid. (GDPR), Article 58 (2) (b).
\textsuperscript{113} Ibid. (GDPR), Article 58 (2) (a).
\textsuperscript{114} Ibid. (GDPR), Article 58 (2) (i).
\textsuperscript{115} Burton, Supra note 18, p. 637.
\textsuperscript{116} GDPR, Supra note 3, Article 32 (1).
of implementing such measures, the state of the art of the measures, as well as several aspects of the processing when considering which security measures will be appropriate for the specific processing operation. Importantly, controllers and processors need to appreciate the risk posed to the rights and freedoms of data subjects when determining the appropriate security measures.\textsuperscript{117}

The Article provides a non-exhaustive list of measures that might fulfil the security requirement, like pseudonymisation and encryption,\textsuperscript{118} the ability to ensure key aspects of cybersecurity,\textsuperscript{119} restoration capabilities\textsuperscript{120} and processes linked to testing and evaluating such measures.\textsuperscript{121} Furthermore, it also sets out a series of scenarios that may be useful when determining the level of security needed to address the relevant risk posed by the processing operation.\textsuperscript{122}

3.2.6 Article 34 – Communication of a Personal Data Breach to the Data Subject

In the security context of the GDPR, it is relevant to look at the obligations on data controllers and processors in relation to data subjects where a data breach has occurred. The GDPR has a codified obligation to notify data subjects where there is a data breach with a high risk of impacting their rights and freedoms.\textsuperscript{123} The affected entities must notify the affected data subjects without undue delay, and in a manner that is easy to understand.\textsuperscript{124} The article affords the data subjects a right of information, a central principle in the EU.\textsuperscript{125} Notably, this notification obligation only applies to controllers.\textsuperscript{126}

\begin{itemize}
\item \textsuperscript{117} Ibid. (GDPR), Article 32 (1).
\item \textsuperscript{118} Ibid. (GDPR), Article 32 (1) (a).
\item \textsuperscript{119} Ibid. (GDPR), Article 32 (1) (b); Namely, the confidentiality, integrity and availability (CIA), as well as resilience of systems.
\item \textsuperscript{120} Ibid. (GDPR), Article 32 (1) (c).
\item \textsuperscript{121} Ibid. (GDPR), Article 32 (1) (d).
\item \textsuperscript{122} Ibid. (GDPR), Article 32 (2).
\item \textsuperscript{123} Ibid. (GDPR), Article 34 (1).
\item \textsuperscript{124} Ibid. (GDPR), Articles 34 (2) and 12 (1).
\item \textsuperscript{126} Burton, Supra note 21, p. 659.
\end{itemize}
It also sets out a series of derogations from the obligation to notify data subject. These deroga-
tions are allowed where there are appropriate technical and organisational measures in
place,\textsuperscript{127} where measures have been taken to mitigate the possible risks to the rights and free-
doms of data subjects,\textsuperscript{128} and where a notification would incur a “disproportionate effort”.\textsuperscript{129} Yet if such an effort would be considered to be disproportionate, the controllers need to either communicate the breach publicly, or through a method that would be equally as effective.\textsuperscript{130}

The GDPR does not delineate the difference between the notion of \textit{risk} mentioned in Article 33 or \textit{high risk} mentioned in Article 34. The lack of a clear distinction and definition of what constitutes a \textit{risk} versus a \textit{high risk} will be discussed and criticised in part 3.4.5., where it will be argued the absence of such a definition or clarification of the differences between risk and high risk is a serious impediment to the practicality of the notification obligation in the GDPR.

\textbf{3.2.7 Article 83 – General Conditions for Imposing Administrative Fines}

As mentioned previously, non-compliance with the GDPR’s security obligations can incur substantial economic consequences. This statement is not an over-exaggeration as Article 83 sets out that an entity infringing the Regulation may be subjected to a fine of up to 10,000,000 euro, or up to 2\% of the total worldwide annual turnover, prioritising the outcome that generates the higher fine.\textsuperscript{131} This number may decrease if there exist some mitigating factors, but working with the possibility of such a fine for non-compliance, gives credence to the fear of the GDPR “beast”. This will be further examined in part 3.4.6.

\textbf{3.3 The Intricacies of the Security Provisions Throughout the GDPR}

The previous part provided an overview of some of the relevant legislative provisions in the GDPR, with a focus on setting out in detail the security provisions of the Regulation. Yet as presented in the introduction, the GDPR is a comprehensive and intricate legal instrument. It is therefore relevant to assess how security permeates the GDPR as a whole and identify pos-

\textsuperscript{127} GDPR, \textit{Supra} note 3, Article 34 (3) (a).
\textsuperscript{128} \textit{Ibid.} (GDPR), Article 34 (3) (b).
\textsuperscript{129} \textit{Ibid.} (GDPR), Article 34 (3) (c).
\textsuperscript{130} \textit{Ibid.} (GDPR), Article 34 (3 (c).
\textsuperscript{131} \textit{Ibid.} (GDPR), Article 83 (4).
sible overlaps and connections across the Regulation on a general basis, as well as how the different provisions interconnect with the data breach notification obligation.

Firstly, a reference to security and adequate technical and organisational measures is made throughout the Regulation, creating a clear indication that security is a central part of the Regulation. Security is set out and referenced in Recitals and Articles alike, enabling a further elaboration of the security requirements and obligations set out in Articles 32 to 34. The following analysis will both look at both explicit and implicit references to adequate security throughout the Regulation.

Adequate security is set out as one of the core principles relating to the processing of personal data, as set out in Article 5 (1)(f). This interlinks with Article 5 (2), which sets out the accountability principle for controllers by requiring controllers to be able to demonstrate compliance with the core principles in the Regulation. Furthermore, one can argue that security is inherently a part of the principles of data minimisation set out in the Regulation, with the rationale being that minimising the processing of personal data might result in less security risks.

Adding to the aforementioned provisions, security is elaborated as one of the key responsibilities of the controller. Article 24 (1) obligates controllers to put in place security measures in line with the security obligations in the Regulation, tying the requirement set out in Article 32 with the obligations enumerated in Articles 33 and 34.

Additionally, Article 34 is explicitly referenced in Article 12 dealing with communication to data subjects. Consequently, where there is a data breach triggering the obligation in Article 34, the information to be communicated to the data subjects needs to be in a “concise, transparent, intelligible and easily accessible form, using clear and plain language”. This adds to

---

132 Burton, Supra note 18, p. 637; GDPR, Supra note 3, Recitals 2, 39, 49, 71, 78, 81, 83, 94; Articles 5 (1) (f), 28 (3) (c), 30 (1) (g) & (2) (d), 35 (7) (d) & (9), 40 (2) (h), 47 (1) (d), 70 (1) (g).
133 Ibid. (GDPR), Article 5 (1) (f).
134 Ibid. (GDPR), Article 5 (2).
135 Ibid. (GDPR), Article 5 (1) (c).
136 Ibid. (GDPR), Article 24 (1).
137 Ibid. (GDPR), Article 12 (1).
the rights of data subjects, facilitating understanding of the data breach notification, which consequently expands on the Article 34 obligation, underlining the vital role security plays in the Regulation.

There can also be said to be a link between the obligation to perform a Data Protection Impact Assessment (DIPA)\(^{138}\) and the obligation to communicate a data breach to affected data subjects.\(^{139}\) Seeing as the DPIA needs to be performed when there is a proposed processing activity which may result in a high risk to the rights and freedoms of data subjects, it may tie into Article 34, seeing as both provisions deal with high risk to data subjects. It might be argued that as Article 34 deals with high risks posed by a data breach, and seeing as the DPIA concerns high risks stemming from the processing operation, the notion of high risk may be applicable to both Articles, as a processing operation deemed high risk might equate to a high risk to data subjects if a data breach occurred. However, a processing activity which falls short of the requirement of a DPIA might still trigger the notification obligation in Article 34 as the ex-post requirement of the notification obligation might uncover a high risk to the data subjects after processing has ensued. This discussion further underlines the security focus of the Regulation.

Article 25 also encompasses a security perspective when it comes to the obligation concerning data protection by design and by default.\(^{140}\) The Article sets out an obligation on controllers to ensure undertaken processing activities are designed to be privacy friendly to the highest extent, with a clear security focus, in ensuring appropriate technical and organisational measures are in place by default.\(^{141}\) It also sets out that the processing operations shall ensure the principle of data minimisation is upheld and that the data is secure.\(^{142}\) One can argue that Article 25 as such provides for an obligation to ensure security by design and by default, in the context of data protection. This is based on the fact that the prescribed approach to data protection by design and by default ultimately revolves around the controller ensuring that appropriate security measures are in place. Article 25 arguably ties into the data breach notification obli-

\(^{138}\) Ibid. (GDPR), Article 35 (1).
\(^{139}\) Ibid. (GDPR), Article 34.
\(^{140}\) Ibid. (GDPR), Article 25.
\(^{141}\) Ibid. (GDPR), Article 25 (1).
\(^{142}\) Ibid. (GDPR), Article 25 (2).
gation, seeing as a stronger focus on security by design and default may result in fewer data breaches which pose any risk to data subjects.

It is also relevant to perform an analysis of the interconnectivity between Articles 32, 33 and 34. Firstly, one can argue that Article 33 is an exemplification of Article 32, since Article 33 presents an obligation stemming from the need to implement adequate security presented in Article 32. Thus, without appropriate technical and organisational measures ensuring adequate security, data breaches will occur without being able to hold the affected entity accountable. Arguably, Article 33 is introduced to clearly deal with a defined aspect of security in the Regulation. The data breach notification obligation is thus a practical approach to regulation, which one can argue is beneficial for affected entities as they enforce the security principle set out in Article 32. The practicality of which will be analysed further in chapter 4. There is also a link between Article 33 and 34. This link is more self-explanatory, as one can argue that where it is deemed necessary to notify data subjects following a data breach pursuant to Article 34, it must also notify the relevant DPA, as the risk level in Article 34 is higher than in Article 33, triggering both data breach notification obligations.

The above analysis has highlighted the vital role adequate security plays in the GDPR, and the way security permeates the various provisions of the Regulation. The following part will set out criticisms related to relevant provisions in the GDPR.

3.4 Critical Analysis of the GDPR

3.4.1 Harmonisation of the European Data Protection Sphere

As argued above, the GDPR is a step in the right direction to further harmonise the data protection legislative framework at the EU Member State level, given the requirement for direct application in Member States. Yet as a first point of criticism, even with the enactment of the GDPR, there is still room for discrepancies to exist within European data protection context. Articles, such as Article 88, dealing with processing in the context of employment, allow the

143 Ibid. (GDPR), Article 34.
144 Ibid. (GDPR), Article 33.
145 As a point of observation, the previously discussed method of presenting a requirement and an ensuing obligation is not only relevant in the security context. Articles 24 and 25 of the Regulation seems to follow the same rationale; Article 24 sets out the responsibilities of the controller, and Article 25 exemplifies it through an obligation to ensure data protection by design and by default.
Member States to enact specific rules within that area.\textsuperscript{146} Such rules add to the scope of the GDPR, reducing harmonisation of the data protection sphere.\textsuperscript{147} Furthermore, as the GDPR does not deal with every aspect of data protection, Member States enjoy the freedom to freely legislate in the areas which are not covered by the Regulation.

As the Regulation is a comprehensive and complex legal instrument, one line of critique in relation to the GDPR harmonisation efforts is that the GDPR lacks guidance on how it is to be interpreted.\textsuperscript{148} Consequently, there may be some divergence in how the GDPR has been translated into national laws; some countries may enact stricter standards than set out in the Regulation, reducing harmonisation.\textsuperscript{149} Some Member States have actively been doing this by enacting specification clauses within the GDPR.\textsuperscript{150} They have consequently legislated more specifically within certain areas of data protection.\textsuperscript{151} Naturally, this may lead to Member States and affected entities interpreting the Regulation in wholly different ways, leading to discrepancies in the harmonisation efforts of the EU within data protection. Conversely, the EU commission has underlined that Member States should avoid enacting legislation that go above and beyond the GDPR, to ensure a better harmonised EU wide legislative framework.\textsuperscript{152} That said, the GDPR has only been in force since 2016; therefore, it is still too soon to take a definitive stance on the state of harmonisation of data protection in EU Member States.\textsuperscript{153}

3.4.2 Rights of Data Subjects and Transparency

Recital 7 of the GDPR states that data subjects should have control of their personal data. Seeing as data breaches are to be communicated in a clear and understandable manner to the data

\textsuperscript{146} Ibid. (GDPR), Article 88; Von dem Bussche & Zeiter, \textit{Supra} note 44, p. 581.
\textsuperscript{147} Ibid. (Von dem Bussche & Zeiter), p. 581.
\textsuperscript{149} Burton, \textit{Supra} note 18, p. 633.
\textsuperscript{151} Ibid. (Multistakeholder Expert Group), p. 27.
\textsuperscript{152} EU Commission, \textit{Supra} note 8, p. 7; Ibid. (Multistakeholder Expert Group), p. 6.
subjects, one could assume that this enhances the rights of data subjects in relation to data breaches. This conception is somewhat naïve as it is unlikely to give the data subjects any meaningful control over their personal data following a breach. Even if one is alerted to a data breach concerning one’s personal data, or there is data processing contrary to the GDPR, it is unlikely that data subjects will have the knowhow to be able to adequately deal with the possible consequences of the breach, creating a false sense of control stemming from transparency.

3.4.3 Article 32 - Security

One of the criticisms of Article 32 is that the phrasing requires implemented security measures to be appropriate to the risk posed. Determining which security measures are to be deemed appropriate in any given processing operation requires an extensive analysis on the part of the controller or processor. As Burton elaborates, by using the word appropriate, it “indicates that controllers and processors must identify the situation-specific risks, assess their potential impact having regard to the particular circumstances of the processing and implement measures to mitigate (at least) those risks which are the most likely to materialise and those whose impact would be the most severe”. Controllers and processors alike may not necessarily have the relevant expertise to be able to fully comprehend the extent of their processing operations.

A way to determine and aid entities in the risk-based assessment outlined above, where one determines which measures would be appropriate in the context of the processing operations, could be to follow a pre-defined standard like the ISO 27001. Arguably, it would serve as an appropriate security standard. The ISO 27001 concerns the implementation of an Information Security Management System, which tackles key cybersecurity concerns and includes defined measures to achieve a level of security. Furthermore, as Diamantopoulou et al states, the “ISO 27001 and GDPR aim both to strengthen data security and mitigate the risk

---

154 GDPR, Supra note 3, Article 12.
156 Burton, Supra note 18, at p. 635.
of data breaches, and they both require organisations to ensure the confidentiality, integrity and availability of data”.  

Following this line of argument, adherence to the ISO 27001 could be argued to signify compliance with the GDPR at a certain level, as well as facilitating entities’ compliance with the security obligations in their own way through their management system. However, the standard is comprehensive and requires a substantial amount of human and financial resources to implement, which may deter entities from implementing it in a data protection context. This highlights the argument that the risk-based approach in the GDPR does not necessarily provide for a more practical way of dealing with security without further guidance.

Additionally, the vague, limited and arguably broad examples of what may amount to risk provided in the Article may also result in entities precluding future risks, which may include the possibility of the risk of physical harm, seeing as unlawfully disclosed personal information can be used to target vulnerable data subject. As such, there is a clear need to further define the concept of risk in relation to the GDPR.

Article 32 also sets out a series of scenarios and some specific techniques that would qualify as adequate security following the Regulation. Seeing as the Article deems those measures to be considered suitable to fulfil the security requirement, it is reasonable to assume that such measures are preferable when ensuring adequate security, placing a degree of expectation on controllers and processors to implement them where possible. However, by explicitly mentioning techniques like encryption, entities may see it as a solution to all their security problems, since it is explicitly referenced. That may not be the case. Encryption is not infallible; it may have flaws. It has been argued that encryption may be less effective when considering data in motion. Furthermore, it suffers from the same fallacy as all technology, it is only as

---


163 See further discussion in part 3.4.5.

164 Burton, Supra note 18, p. 636.
secure as its weakest link. Encryption might also become a less secure technology in the future, as quantum computing will likely be able to break traditional encryption measures, making the reference to encryption as an adequate measure questionable. However, to date, encryption is considered to be a strong technology ensuring adequate security, and the criticism set forth by the Article 29 WP that encryption will become less secure in the future may be unfounded. Quantum computing may also bring with it stronger encryption measures, making state of the art encryption a viable option for mitigating data breaches.

3.4.4 Article 34 – Data breach Notification to Data Subjects
A significant criticism of Article 34 is that the listed exceptions for notification might make notifications to data subjects a rarity. As the rationale behind the Article arguably lies in that ensuring affected data subjects are made aware of a data breach, the sooner they are able to take steps to mitigate or reduce the possible high risk, the more likely derogation from the obligation becomes disharmonious.

In the national implementation of Article 34, some Member States developed their own requirements and guidelines to deal with notifications to data subjects. One might argue that such national initiatives to further define the obligation to notify data subjects makes a case for the obligation being too vague. This may in turn lead to a lesser degree of harmonisation within the notification obligations, which in turn may cause legal uncertainty for entities. The efforts taken by Member States can be seen as a signal that there is a clear need to further define the obligation in Article 34.

165 Winn, Supra note 67, p. 1146.
168 Article 29 WP, Supra note 106, p. 19.
170 Grimes, Supra note 167, p. 126.
171 De Hert & Papakonstantinou, Supra note 76, p. 191.
3.4.5 The Notion of Risk and High Risk in Articles 33 and 34

A key criticism central to this thesis is the absence of a clear definition, clarification, guidance or jurisprudence concerning what constitutes risk and high risk in the GDPR. Even though the Regulation does somewhat define what constitutes as possible risks to the rights and freedoms of data subjects, there is no common understanding in the data protection legislation of what the concept of risk is and it does not deal with the notions of risk versus high risk. The rationale behind having a distinction between risk and high risk when it comes to notification to data subjects is that if all breaches were to be reported to the affected individuals, it may cause what is known as “notification fatigue”. Notification fatigue is where over-notification of data breaches to affected individuals desensitises the data subjects to the possible adverse effects of the data breach. It is therefore pertinent to have a distinction between breaches causing a risk and high risk to avoid notification fatigue. There may, however, arise an issue where the controller is unsure of whether there is a risk or a high risk, as well as there being a disproportionate effort in contacting all the affected data subjects, which will result in the possibility of unnecessary public notifications that might further damage the entities reputation. As Jakobi et al states: “this law is about controlling the risks that arise for people when data that relates to them is processed”, it is therefore paradoxical that there is no further explanation of the risk thresholds. Entities might get some guidance if a DPIA has been conducted, as the processing activities have already been deemed as high risk. Yet the issue at hand is whether the data breach, not the processing activities, causes a high risk or a risk to data subjects. The DPIA can certainly be of guidance where it has been performed, but it may not necessarily indicate that the data breach itself poses a high risk.

---

175 Article 29 WP, Supra note 106, p. 20.
To summarise, the fact that there is no definite definition of risk and high risk is a hinderance to effective exercise of the obligations in the Regulation and a source of confusion.\textsuperscript{179} Entities like the EDPB or the CJEU should develop a narrative that clearly delineates when there is a risk and a high risk,\textsuperscript{180} which interestingly is part of the EDPB’s tasks, but has not yet been undertaken.\textsuperscript{181} As such, the argument presented in this part stresses the fact that as it is difficult for entities to delineate the risk thresholds, the lack of elaboration on how to determine the different thresholds lessens the degree of practicality of the data breach notification obligation.

3.4.6 Article 83 - Fines

On the positive side, the possibility of a hefty fine might ensure entities are more conscious of their own security practices, incentivising them to update such practices as technology develops and threat actors find new ways of performing data breaches.\textsuperscript{182} Yet one can contemplate the real effect of the threat of economic sanctions. The DPA in the United Kingdom has suggested that for less serious breaches, it will not impose a substantial fine. The reality may be that entities may refrain from implement rigorous security, as they are aware that less serious breaches will not result in a fine, which may fail in deterring non-compliance.\textsuperscript{183} Were such a practice to become the norm, it might lessen the impact of the GDPR when it comes to non-compliance of the security provisions, if the only real compliance measure under the GDPR are hefty fines. If the quanta of fines becomes negligible, it will be cheaper for entities to pay the fine, rather than implementing adequate security. For the fines to be an effective deterrent, is seems unlikely that they need to be that of the maximum set out in Article 83.\textsuperscript{184} Fines need to be at a level that makes it financially beneficial to implement rigorous security practices,\textsuperscript{185} meaning that the fine must be greater than the possible economic impact of implementing the

---

\textsuperscript{179} Multistakeholder Expert Group, \textit{Supra} note 150, p. 4.
\textsuperscript{180} \textit{Ibid.} (Multistakeholder Expert Group), p. 36.
\textsuperscript{181} GDPR, \textit{Supra} note 3, Article 70 (1) (h).
\textsuperscript{183} Hedley & Jacobs, “The Shape of Things to Come: The Equifax Breach, the GDPR and Open-Source Security”, \textit{Computer Fraud & Security} (November 2017), p. 6
relevant security measures. Consequently, the GDPR may give too much leeway for DPAs when determining the level of a fine, reducing the quanta to a point in which it is no longer a deterrent.

On the other hand, the possibility of a hefty fine gives rise to the argument that the GDPR contains more ‘sticks than carrots’ when considering regulatory compliance. Although it is instrumental to have option to impose fines, it might be preferable to have better incentives besides the fear of economic sanctions for non-compliance with the GDPR. The corrective powers of the DPAs, like the ability to stop processing activities,\textsuperscript{186} may in fact be a more effective deterrent.\textsuperscript{187} However, one can say that the possibility of large economic sanctions does act as an indirect incentive to improve one’s security, as entities are more likely to invest in adequate security measures when the possibility of large sanctions outweigh the cost of implementation of such security measures.\textsuperscript{188}

The following part addresses the broader subject of the fact that one cannot achieve the aim of the GDPR without adequate security. Additionally, it conducts an overall analysis of security in the GDPR as it provides a relevant backdrop for the ensuing discussion concerning the interpretative and practical problems posed by the data breach notification obligation.

\textbf{3.5 Security in the Data Protection Context}

As a starting point, Vanberg states: “(...) data protection laws are indeed welcome instruments in protecting privacy in the online sphere, but they cannot be sufficient on their own without vigilant and well-informed consumers as well as companies/organisations who are constantly reviewing and improving the security of user data”.\textsuperscript{189} One can argue that it is near impossible to achieve the aim of the GDPR without adequate security. This is based on the fact that data subjects have no meaningful control over their personal data. Arguably, they have no way of implementing security measures protecting their personal data themselves. Legislation, such as the GDPR, therefore requires the entities processing personal data to en-

\textsuperscript{186} GDPR, \textit{Supra} note 3, Article 58 (2) (f).
\textsuperscript{187} EU Commission, \textit{Supra} note 8, p. 5.
\textsuperscript{188} Schneier, \textit{Supra} note 185.
sure appropriate security seeing as data subjects cannot do so themselves.\textsuperscript{190} However, one can argue that even if we had data protection laws that went above and beyond the GDPR, it might still be insufficient to protect the rights and freedoms of data subjects.\textsuperscript{191} Data breaches will always exist and therefore undermine personal data of data subjects.\textsuperscript{192} Threat actors conducting data breaches will always be a significant risk to data subjects.\textsuperscript{193}

It is important to point out that as the security provisions in the GDPR concern \textit{appropriate} technical and organisational measures, it does not mean that every entity suffering from a data breach would be in breach of the GDPR.\textsuperscript{194} Even if the entity has taken appropriate steps\textsuperscript{195} to secure its data, the threat actors may still have found a way to work around it, thus signifying compliance with the Regulation even though a data breach has occurred.\textsuperscript{196} The discussion of appropriate measures is relevant as the GDPR as such does not require the implementation of \textit{perfect} security. In our highly digital society, there will always be threat actors that can find a way into an entity’s system. As Brusci argues: “\textit{Unfortunately recent trends in the computer attack field show that even the adoption of strongest cybersecurity protection measures cannot be enough for avoiding data breaches}”\textsuperscript{197}. This inevitability of data breaches does not mean that one can slow down in the efforts to implement security measures. The security provisions in the GDPR will therefore require that there is at least a base-level of implemented security, which in turn might hopefully slow threat actors down, or permit action to be taken.

After the enactment of the GDPR, media interest in security and data breaches has increased. It can be argued that this is based on the fact that the value of personal information has seen an unprecedented increase,\textsuperscript{198} coupled with the rising risk of its misuse\textsuperscript{199} and the need for the

\begin{itemize}
  \item Burdon, Lane & von Nessen, \textit{Supra} note 162, p. 297.
  \item Vanberg, \textit{Supra} note 189, p. 20.
  \item \textit{Ibid.} (Vanberg), p. 20.
  \item \textit{Ibid.} (Vanberg), p. 20.
  \item Burton, \textit{Supra} note 18, p. 637.
  \item This raises the question of whether it is sufficient for entities to demonstrate that \textit{reasonable steps} have been taken in order to ensure adequate security measures are in place, a discussion which is outside the scope of this thesis.
  \item Bruschi, \textit{Supra} note 158, p. 1.
\end{itemize}
public to be informed of improper security practices concerning personal data. Specific to the enactment of the GDPR, the possibility of substantial financial repercussions for non-compliance further increased the media’s attention when it comes to security incidents concerning personal data. This may be a result of the interest the public has in, firstly, being informed about data breaches which may affect themselves, and to secondly, being a novelty for security conscious data subjects in following the possible data breaches of companies.

Interestingly, when entities are faced with GDPR compliance efforts, they tend to address the obvious compliance issues, for example contracts and newsletters. Following the same line of reasoning when it comes to compliance with the security provisions in the Regulation, one can assume entities will address the most obvious security faults, but not necessarily the most effective ones. Even as the Regulation sets out a series of security measures that are deemed appropriate, some of those measures, such as encryption, are resource heavy to implement, potentially underlining the argument that entities will only deal with the most apparent security faults, making their efforts fall short of the actual requirements of the GDPR.

It may be argued that the data subjects themselves may not be able to fully appreciate the trade-off required to fulfil relevant security obligations. Notably, they might prefer a solution that is more privacy invasive, as the functioning of the technology might be more to their liking (ie. personalisation), based on the fact that they are unable to appreciate the risks posed. Furthermore, data subjects might still use the services of entities that have been the victim of a data breach, even after it is public knowledge as they prefer their services to others. This knowledge-gap is difficult to bridge, and there should be an enhanced focus from entities processing personal data to explain the ways they utilise their data and their security measures. However, as the focus on security when it comes to the processing of personal data continues to increase, one can hope that this will improve accordingly. One might be able to bridge the gap slowly but surely as data subjects become increasingly tech savvy; coupled with the increased media attention on security, this may help educate individuals on the possible risks

199 Burdon, Lane & von Nessen, Supra note 162, p. 297.
201 Winn, Supra note 67, p. 1151-1152.
posed by the processing of personal data. One can hope that data subjects will make better decisions pertaining to who they entrust with their personal data.

All in all, in the realm of security, one could argue that the GDPR advocates for a more proactive approach than previous data protection legislation. The rationale is that the security provisions enable entities to, where possible, avoid data breaches on the basis of appropriate security measures, or where a breach occurs, at least be able to react appropriately. This, coupled with the possibilities of the risk-based approach taken in the Regulation, may provide for, to a certain extent, an adequate legislation when it comes to security and data protection.

### 3.6 Summary

This Chapter has sought to give an in-depth understanding of the relevant provisions in the GDPR, with a deep dive into the more relevant security provisions. The GDPR is, as stated previously, a complex Regulation that has a significant degree of interconnectivity. It is certainly challenging for entities processing personal data to demystify the Regulation, and with its comprehensive text, it is no wonder that entities fear the GDPR’s repercussions. The security provisions in the Regulation cannot be considered clear cut, to its detriment. It has also provided an overarching analysis addressing the concept of security and the GDPR, stating that the GDPR does not require perfect security. It has also stressed that individuals are not necessarily keen on the idea to compromise digital services to receive a more privacy friendly option. However, with adequate public awareness and the increasing media attention, this trend might turn and hopefully, security conscious data subjects will be more aware and appreciative of data protection tenets.

### 4 The Data Breach Notification Obligation in the GDPR

#### 4.1 Overview

As stated in the introduction, data breaches are a relatively common occurrence, carrying with them the possibility of substantial financial, organisational and reputational consequences. Having a codified data breach notification obligation that spans the whole of the EU, setting a global standard based on the GDPR’s wide territorial reach, is therefore a crucial step in the right direction, making it a priority for entities processing personal data.

---


However, even though the data breach notification obligation can be argued to be a good tool for increasing security in the realm of data protection, it remains an imperfect solution for tackling the complex issue of data breaches. This chapter provides a legislative analysis of the data breach notification obligation provision in the GDPR, highlighting its interpretative problems. It then goes on to assess the interpretative and practical problems posed by the data breach notification obligation in the GDPR, as well as proposes ways in which it can be improved in the future.

### 4.2 Legislative Analysis of Article 33 - Notification of a Personal Data Breach to the Supervisory Authority – and Interpretative Problems

The essence of the obligation set out in Article 33 is to notify the relevant DPA where there is a data breach concerning personal data, which poses a risk to the rights and freedoms of data subjects.\(^{205}\) The Article further sets a time restriction as to when the notification needs to be submitted to the DPA (72 hours or without undue delay).\(^{206}\) Where there has been a delay in notification outside of the defined timeline, the notification needs to be accompanied by reasons for the delay.\(^{207}\) Yet how the reasons for delay are to be treated by the DPA, with the possibility of them being discarded and the entity subsequently being found to be in non-compliance of the Article, is unclear and can be seen as an interpretative problem.

Importantly, the Article also sets out the relevant information that needs to be communicated to the DPA when there is a breach resulting in a risk to the rights and freedoms of data subjects. A notification needs to contain a description of the nature of the breach\(^ {208}\), as well as an approximation of the number of data subjects affected by the breach,\(^ {209}\) contact information,\(^ {210}\) a description of possible consequences\(^ {211}\) and measures that have or may be taken in order to address the breach, including possible measures taken to mitigate the adverse ef-

\(^{205}\) GDPR, *Supra* note 3, Article 33.

\(^{206}\) *Ibid.* (GDPR), Article 33 (1).

\(^{207}\) *Ibid.* (GDPR), Article 33 (1).

\(^{208}\) *Ibid.* (GDPR), Article 33 (3) (a).

\(^{209}\) *Ibid.* (GDPR), Article 33 (3) (a).

\(^{210}\) *Ibid.* (GDPR), Article 33 (3) (b).

\(^{211}\) *Ibid.* (GDPR), Article 33 (3) (c).
The Article allows for information that is unable to be communicated at the time of notification to be presented in phases to the DPA, without undue delay. When it comes to the differentiation of a controller and a processor and their respective obligations, a controller needs to notify the DPA of a data breach, whilst a processor obligated to establish whether a breach has taken place and to subsequently notify the controller. Exceptionally, where stipulated in the contractual agreement between the controller and the processor, the processor may notify the DPA on behalf of the controller.

Entities experiencing data breaches require documentation that their security systems are capable of dealing with data breaches, as well as notifying the relevant DPA and possibly affected data subjects. The Article 29 WP goes further than the obligation to keep records of processing activities in the GDPR, and recommends entities should, in addition, retain a record of decisions made in relation to a data breach. This further ties into the requirement to keep records of processing activities in Article 30, which states relevant entities should set out a general description of their security measures, “where possible”. The vague formulation of “where possible” may be a hindrance to effective data breach notification and mitigation, as this information can be instrumental when dealing with breaches. As such, it should be a requirement to be able to show compliance with the security requirements set out in the Regulation. This would make data breach notification less burdensome, as it would be easier for entities to compile the necessary information about the data breach from a combination of the records of their processing activities and their security measures.

The Article therefore places a heavy burden on the controller when it comes to gathering the relevant information that needs to be communicated, an aspect of the data breach notification that may be argued to place a disproportionate burden on affected entities when viewed in tandem with the pre-defined time-limitation for notifying a breach.

212 Ibid. (GDPR), Article 33 (3) (d).
213 Ibid. (GDPR), Article 33 (4).
214 Article 29 WP, Supra note 106, p. 13.
216 Burton, Supra note 21, p. 649.
217 GDPR, Supra note 3, Article 30.
218 Article 29 WP, Supra note 106, p. 27.
4.3 Practical Difficulties Related to the Data Breach Notification in the GDPR

One practical problem when it comes to the data breach notification obligation is the aforementioned time-limit.\(^{219}\) In practice, entities suffering a data breach may be unable to collect the information required to be included in the notification within the stipulated time-limit, causing it to fall short of the legislative requirement.\(^{220}\) Seeing as some of the technology employed to gather the relevant information about the data breach may take as long as 72 hours, or longer, to compile,\(^{221}\) this is a serious flaw in the pre-defined time-limitation under Article 33. Even though the Article enables some leeway in that entities may provide the relevant information in phases, without further undue delay, it is unclear how the DPAs will interpret what constituted undue delay. Furthermore, it is also uncertain whether the DPAs have the relevant competence needed to appreciate why the technical solutions might take longer than the pre-defined time-limit to compile the information. This in turn poses a clear interpretative and practical problem when assessing the data breach notification obligation.

Additionally, the Article 29 WP has suggested that entities experiencing a data breach should conduct a short investigation with the aim of establishing whether or not a breach has occurred.\(^{222}\) During the investigation period, they argue that the entity is not to be considered to be “aware” of the breach, pursuant to Article 33, which may give some leeway in collecting the relevant information concerning the breach.\(^{223}\)

Furthermore, if the entity becomes aware of the data breach and it is still in progress, the time-limit in the GDPR may not be complied with as the efforts of the entity might be focused on mitigation and/or stopping the breach, rather than ensuring compliance.\(^{224}\) Consider a large entity that experiences a data breach concerning a magnitude of data subjects; requiring publicly notification may alert the threat actors to the fact that the affected entity is aware of the on-going data breach, thereby compromising attribution or mitigation efforts.

---

\(^{219}\) GDPR, Supra note 3, Article 33 (1).
\(^{220}\) O’Brien, Supra note 157, at p. 83.
\(^{221}\) Wilson, Supra note 182, at p. 10.
\(^{222}\) Article 29 WP, Supra note 106, p. 11.
\(^{223}\) Ibid. (Article 29 WP), p. 11.
\(^{224}\) Esayas, Supra note 125, at p. 322.
4.4 Purposely Withholding Notification of an Ongoing Data Breach as a Mitigation Measure

Building on the preceding issue concerning the practicalities of the data breach notification obligation, it is pertinent to assess the possibility of entities purposely withholding notification of an ongoing data breach as a mitigation measure.\(^{225}\) When a data breach occurs, the entity might deem it vitally important to keep the knowledge of the ongoing breach secret, to prevent the threat actors from becoming aware that the entity is informed of the ongoing situation whilst they work to attribute the breach and to implement security efforts to mitigate its effects.

Furthermore, if the ongoing breach becomes public knowledge, other threat actors may try to take advantage of it by performing their own data breaches on an already compromised system, supporting the need for delaying the notification of the breach.\(^{226}\) The entity may therefore be in non-compliance with the Regulation if the efforts of attribution goes beyond the 72 hours required in the Regulation. In this scenario, non-disclosure of the breach will therefore be a key security effort, whilst at the same time, acting contrary to the notification obligation in Article 33, highlighting the practical problems tied to the Article.

4.5 Over-Notification of Data Breached to DPAs and Notification Fatigue

Over-notification is a serious issue that needs to be addressed in the context of the data breach notification obligation. Over-notification has two aspects, the over-reporting of low-risk data breaches to (1) DPAs and to (2) data subjects. This can be argued to be a result of a lack of a set definition of risk to the rights and freedoms of data subjects, and a lack of further elaboration of what constitutes risk and high risk in the GDPR, as set out previously in part 3.4.5.\(^{227}\) Both situations may be a result of entities suffering a personal data breach notifying either the DPA or the data subjects out of an abundance of caution.\(^{228}\) In turn, this may be based on the

\(^{225}\) Such as the Australian National University, which spent two weeks from becoming aware of the breach until they notified the breach, as they prioritised introducing security measures to mitigate the effects of the breach and prevent subsequent breach attempts (Australian National University, *Incident Report on the Data Breach of the Australian National University's Administrative Systems*, Public Incident Report (2019), p. 2).


fact that the entities fear the possible fines imposed for non-compliance, and would rather notify one time too many than one time too few.

Over-notification of low-risk data breaches to DPAs can have adverse consequences, including undermining the legitimacy of the GDPR, as DPAs often suffer from a lack of funding. As a consequence, over-notification may deplete DPAs resources, since DPAs are obliged to process all data breach notifications that they receive, regardless of their level of risk. The tying up of resources to deal with low-risk data breach notifications are arguably a significant cause for concern, as DPAs have several other functions addressing data breach notifications. This is especially worrisome, as some DPAs have reported a substantial increase of data breach notifications, causing a two to three-fold increase in their case load since the introduction of the GDPR’s mandatory notification obligation.

Notification fatigue, as set out in part 3.4.5, is a real risk when it comes to the data breach notification obligation. The main concern is, as entities may have difficulty determining which data breaches need to be communicated to the data subjects, they will notify where it is not required, again, just to be cautious. This might result in data subjects being desensitised to the risk posed by data breaches, reducing the possible positive effects of the notification obligation on data subjects. As seen from the line of argument above, more notifications of data breaches do not necessarily equate to better security and protection for data subjects. To avoid notification fatigue, there needs to be better understanding of which data breaches ought to result in notification, based on a risk-assessment and guidance from the relevant EU authorities elaborating the differentiation between “risk” and “high risk”.

The arguments presented above highlight a main issue tied to the data breach notification obligation, underlining that even though the risk-based approach taken in the GDPR marks posi-
tive progress towards a more practical approach, it requires further elaboration and clarification seeing as there are clear interpretative and practical problems tied to the obligation in relation to over-notification.

4.6 Analysing Risks to the Rights and Freedoms of Data Subjects

Tying into the preceding argument, one must also consider the difficulties entities may face in establishing whether there is a risk to the rights and freedoms of data subjects. Most entities are used to performing risk analysis from a business perspective. As such, the risk analysis required to be able to appreciate the risks posed to data subjects may be quite foreign as opposed to their own perception of risk based on business risk analysis. Even though the GDPR does set out what such risks can include, this risk analysis still presents as a practical problem for personal data processing entities. This further underlines the need to elaborate the risk thresholds in the GDPR, as well as the need to issue guidelines in determining what constitutes a risk to the rights and freedoms of data subjects.

4.7 Purposely not Detecting Data Breaches

Provisions of data breach notifications to DPAs may be indicative as to whether or not the GDPR has been complied with, as the Regulation obligates controllers and processors to implement adequate security. The information provided in the data breach notification, coupled with the records of processing, arguably provide an indication of whether there is compliance with the Regulation. As Article 33 of the GDPR states that notification is to be given when the entity suffering a data breach becomes aware of it, it might result in some entities trying to deliberately not to become aware, or detect, whether or not a breach has occurred. This is problematic as it goes against the rationale of the security Articles in the GDPR and is a clear interpretative problem. The obligation and its possible financial repercussions may therefore lead to entities deliberately choosing to implement poor security, thereby rendering themselves unable to detect data breaches. It is, however, unlikely that many entities will utilise this approach, as the potential of third parties to discover and report data breaches to the attention of the public and the DPA may provide adequate discouragement.

---

236 GDPR, Supra note 3, Article 33 (5).
237 Burton, Supra note 21, at p. 632.
238 Nieuwesteeg & Faure, Supra note 13, p. 1241.
ment of such an approach. Even though third parties do not discover the majority of data breaches, the mere possibility of being called out may provide enough of an incentive to put such practices of non-detection to rest.

4.8 Data Breach Notification and the Lack of Security

In the broader security context, it is interesting to address whether one could claim that an entity suffering a data breach does in fact have inadequate security measures in place. As pointed out above, we are progressing towards a digital society where it is only a question of when, not if, an entity will suffer a data breach. However, a data breach in itself does not necessarily constitute a lack of security. It is therefore pertinent to address that the failure to notify a data breach is a strong indication that there is a lack of security in the entities concerned, as it may be an indication that the entity is in non-compliance with the Regulation.

Additionally, it may be the case that it is in fact the entities which have adequate security in place that are able to detect the data breaches, compared to those with a lower level of security. This will arguably result in entities with better security being able to notify about data breaches, as opposed to those with lower levels of security; almost 50% of entities experiencing a data breach became aware of it through a routine security check. Thus, if an entity does not have the necessary technical and organisational security measures in place, which are able to detect data breaches, it might lead to entities with better security constituting disproportionate part of the data breach notification statistics. This is inherently a practical problem and concern posed by the obligation.

---

240 Ibid. (Nieuwesteeg & Faure), p. 1241.
241 Burton, Supra note 21, at p. 631.
242 Article 29 WP, Supra note 106, p. 10.
243 Winn, Supra note 67, at p. 1149.
244 Næringslivets Sikkerhetsråd, Marketallsundersøkelsen 2020, Report, 12th edn. (2020) (Authors translation from Norwegian to English), at p. 25.
4.9 Small and Medium-Sized Enterprises and the Data Breach Notification Obligation

A criticism that has often been raised when it comes to the GDPR is its effect on small and medium-sized enterprises (SMEs).\(^{245}\) Representatives from SMEs have raised the issue that to be in compliance with the obligations in the GDPR, they must expend considerable resources. This is a significant issue, as they often lack adequate economic and human resources to implement the GDPR’s obligations.\(^{246}\) This criticism can be extended to the data breach notification obligation, as they often lack qualified security personnel and resources to deal with the data breach notification obligation,\(^{247}\) posing a significant practical problem for SMEs.

Based on the interpretative problem posed by the lack of a clear definition of what constitutes a risk or high risk to data subjects, SMEs are in a particularly difficult position when it comes to the data breach notification obligation. Additionally, the time limitation imposed further adds to the challenges of SMEs, as they often lack an adequate security framework and may therefore be dependent on other security entities to compile the necessary information for a notification. SMEs especially require further guidance from the relevant EU authorities on how to assess risks in their processing activities, as well as risk levels in relation to data breaches.\(^{248}\) Furthermore, it could be beneficial for SMEs to receive guidance from the relevant EU authorities concerning outsourcing as a viable option in mitigating the security and notification challenges posed.

4.10 Personal Data Breaches: Reputational Damage or a Competitive Advantage?

Entities experiencing data breaches will often consider that the best course of action is to not notify a personal data breach. This may be down to the fear of reputational consequences, including a loss of customers, experience a decline in stock prices,\(^{249}\) or the loss of standing in the competitive environment.

\(^{245}\) Multistakeholder Expert Group, *Supra* note 150, p. 4.

\(^{246}\) Ibid. (Multistakeholder Expert Group), p. 4.


\(^{248}\) Ibid. (ENISA), p. 52.

The issue concerning reputational damage following a data breach may have disproportionate effect on different entities; some entities may not suffer reputational damage at all, whilst others may face bankruptcy upon discovery of a breach.\textsuperscript{250} Interestingly, in a report setting out the digital security environment for Norwegian businesses and some public entities, only 14% of the responding entities reported to having suffered reputational losses following a data breach in the past 12 months.\textsuperscript{251} This impact of a fear of reputational damage is therefore unclear; it may encourage entities to implement better security measures to prevent data breaches,\textsuperscript{252} the impact on their reputation may be negligible.

It is also relevant to consider that adherence to the GDPR might in fact mitigate the possibility of reputational damage if the entity can demonstrate compliance with the Regulation, with an emphasis on the security provisions, as it enables them to communicate what security measures they have in place and to adequately assess which security measures should be implemented.\textsuperscript{253}

Furthermore, openness about data breaches might facilitate a greater understanding posed by the current threat climate to data processing entities, and especially SMEs. Such an openness and willingness to share experiences and breach consequences might become a competitive advantage facilitating transparency in the data protection context.\textsuperscript{254}

\subsection*{4.11 The Role of the Data Protection Authorities}

As stated in part 4.5., DPAs often lack human and financial resources. The lack of resources can undermine the legitimacy of the DPAs, an unfortunate consequence which may ultimately lead the undermining of the GDPR as a whole. As Nieuwesteeg & Faure states, “\textit{Ultimately, if notifications merely end up in a digital drawer at the DPA and no further action is taken to promote data security, then obviously the entire DBNO (Data Breach Notification Obligation) is a failure.}”\textsuperscript{250}

\begin{flushright}
\textsuperscript{250} Nieuwesteeg & Faure, \textit{Supra} note 13, p. 1238.
\textsuperscript{251} Næringslivets Sikkerhetsråd, \textit{Supra} note 244, p. 47.
\textsuperscript{253} Multistakeholder Expert Group, \textit{Supra} note 150, p. 35.
\textsuperscript{254} Voss & Houser, \textit{Supra} note 69, p. 334-337.
\end{flushright}
would become an extremely costly exercise, without any social benefits as far as improving cyber security is concerned”.

As such, the GDPR requires strong enforcement to have the desired impact on the relevant entities, avoiding the undermining of the Regulation based on underenforcement.

Conversely, DPAs are in a prime position to produce guidelines and best practices for how to deal with data breach notifications, as they are the recipient of a substantial amount of data that is highly valuable and necessary to be able to establish such practices. However, as one of the criticisms of the DPAs claims they are unable to provide adequate and timely consultations in the process of a data breach, this might not be possible until they have adequate human and financial resources. As such, there is a need for well-funded DPAs with the will to issue guidelines and best-practices, as well as enforcing the GDPR and reprimanding those in non-compliance, to mitigate the interpretative and practical problems posed by the obligation.

4.12 The Issue of Multiple Data Breach Notification Obligations in EU Law

As set out in part 2.5., the GDPR is not the sole EU instrument setting out a data breach notification obligation. The fact that there are multiple legal instruments dealing with data breach notification in the EU, all with different mandates, may pose a practical problem to entities experiencing a data breach concerning personal data. Entities might have to provide several notifications for one data breach, based on the different aspects of the breach. This is based on the fact that the different legislative instruments dealing with notifications will, on a general basis, set out different requirements as to what such a notification is to be comprised of. As an example, if a trust service provider (for example, a telecoms provider) experiences a breach concerning personal data, it might have to notify under the eIDAS Regulation, the GDPR and the ePrivacy Directive, and the notification might have to be comprised of different information for each notification. The different notification obligations might therefore create serious administrative and financial consequences on the affected entity.

---

255 Nieuwesteeg & Faure, Supra note 13, p. 1245.
256 GDPR, Supra note 3, Recital 7.
257 Multistakeholder Expert Group, Supra note 150, p. 16.
258 Esayas, Supra note 125, p. 321.
259 Burton, Supra note 21, p. 643.
260 Daly, Supra note 86, p. 485.
261 Ibid. (Daly), p. 485; Esayas, Supra note 125, p. 321.
more, as some of these instruments dealing with data breaches are Directives, states enjoy a larger freedom in how those laws are implemented, compared to Regulations.262 This could result in legal uncertainty263 and further economic and administrative burdens. However, with the passing of the GDPR, it might be possible for the EU to reference back to the data breach notification obligation in the GDPR when legislating in the future, improving the harmonisation of the notification landscape.

Additionally, the existence of different notification obligations poses another issue which ties into the data breach notification obligations; whether or not technical and organisational measures required to comply with the GDPR also facilitate compliance with the NIS Directive.264 Both of the legal instruments deal with security and a data breach notification obligations, therefore, it would be beneficial to ascertain if the reference to security would constitute the same under both notification obligations, which would further lessen the legal uncertainty of the overlapping legislations.265

### 4.13 Summary

This Chapter has sought to provide a thorough analysis of the data breach notification obligation and the interpretative and practical problems it poses in the security context of the GDPR. As set out above, it is clear that the obligation is not perfect; there are problems concerning the interpretation and practicality of the obligation, the need for entities to sometimes be in non-compliance with the notification obligation to be able to impose mitigation measures, the issue of notification fatigue and over-notification, detection, security, SMEs, reputational damage, the role of the DPAs, and the challenges posed by different pieces of EU notification legislations. As such, these problems accentuate the overall issue that the risk-based approach taken in the GDPR is not necessarily entirely practical, and that there is a further need to deal with the issues highlighted and provide further guidance.

---

262 Craig & De Búrca, *Supra* note 6, p. 138-139.
263 Wolters, *Supra* note 196, p. 175.
5 Conclusion

Data breaches are inevitable and the attention they now receive has put them on the global agenda. Threat actors are finding increasingly devious ways of penetrating security efforts of entities processing personal data; seeing as personal data is a hot commodity in both legitimate and illegitimate markets. The GDPR and its security requirements for entities processing personal data provides for a first line of defence for data subjects in the digital age. Additionally, the data breach notification obligation in the GDPR acts as a means of keeping entities accountable for their security practices and enables oversight of their compliance with the Regulation by the DPAs.

With the potential for widespread consequences for entities and data subjects alike, it is clear that the data breach notification obligation is a necessity in the realm of data protection. This thesis has sought to answer the research question by exploring the security provisions in the GDPR, in addition to other relevant provisions, in order to create a holistic backdrop for the analysis of the data breach notification obligation and its interpretative and practical problems.

This thesis argues that the data breach notification obligation poses a significant compliance challenge for entities experiencing a data breach, emphasising issues of risk and the lack of a definition of risk threshold in the Regulation. This is a significant challenge to the practicality and interpretation of the obligation; entities may either revert to either over-notification practices or to completely refrain from notifying. Furthermore, the underfunding of DPAs and the possible lack of willingness of those DPAs to fine for non-compliance, may contribute to a less practical means of regulating entities experiencing a personal data breach. When considering the practicality of the risk-based approach, there are issues linked to the data breach notification obligation, specifically, how to perform the necessary risk analysis maintaining the rights and freedoms of data subjects at the core. Another concern is how compliance with the strict time-limit in Article 33 will be interpreted when there may be a pressing need to disregard it to implement mitigating efforts. Adding complication to this consideration is the role of SMEs, and how these entities may provide adequate notification to DPAs and data subjects without disproportionate economic effects. Moreover, the fact that there are multiple

---

266 Wilson, Supra note 182, at p. 8.
data breach notification obligations spanning several EU instruments calls for the need to issue guidelines in how to best navigate the notification landscape by the relevant EU institutions.

It is therefore clear that there is a pressing need to elaborate the risk-conundrum set out in the GDPR. Bodies, like the EDPB, as mandated by the GDPR, should issue guidelines, recommendations and best practices concerning when a data breach results in a high risk to data subjects\textsuperscript{267}, something which is yet to be done. Additionally, the breach notification obligation would benefit from guidance from the CJEU in how to interpret and give guidance on the shortcomings outlined in this thesis. These efforts will aid in unfurling and mitigating issues like that over notification fatigue and possibly, the depletion of DPA resources based on over-notification. In general, there needs to be further efforts on the part of bodies like the EDPB to address the emerging issues linked to the data breach notification obligation. However, it is important to keep in mind that adoption of the GDPR is still relatively recent; it is therefore natural to assume that these may be issued in the foreseeable future.

In conclusion, with further elaborations, guidelines, best-practices, jurisprudence and recommendations tackling the outlined interpretative and practical problems, the data breach notification obligation in the GDPR is a fundamental obligation in the realm of security and data protection.

\footnote{\textsuperscript{267} GDPR, \textit{Supra} note 3, Article 70 (1) (h).}
Table of reference

**EU Legislative Instruments**

**EU**, Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Directive 95/46/EC


**EU**, Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), Regulation 2016/679

**EU**, Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS), Regulation 910/2014


**EU Documents**


**ENISA**, Data Breach Notification in the EU (2011)


The European Parliament, the Council and the Commission, Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation, EU Guide

Books and Chapters


Cielsa, Encryption for Organizations and Individuals: Basics of Contemporary and Quantum Cryptography, Alpress Media LLC (2020)


Journal Articles


Other Sources


Bloor, How Much Is Data Worth? The Value of Your Personal Data, Permission.io <accessible at: https://permission.io/blog/how-much-is-data-worth/>

California Civil Code


