Report:

Scientific research data breach notification obligation

Bernold Nieuwesteeg [a]
Michel van Eeten [b]
Michael Faure [c]

[a] Erasmus Universiteit Rotterdam, Centre for the Law and Economics of Cyber Security (CLECS)
[b] TU-Delft, Economics of Cyber Security Group
[c] Erasmus Universiteit Rotterdam, Centre for the Law and Economics of Cyber Security (CLECS)

29 NOVEMBER 2018

The Dutch Cyber Security Council has asked the partnership consisting of the Economics of Cyber Security Group (TU Delft) and the Centre for the Law and Economics of Cyber Security (Erasmus University) to carry out scientific research into the effect of public reporting of data breaches within the legal framework of the data breach notification obligation in the GDPR.

About the authors:

Mr. dr. ir. Bernold Nieuwesteeg is director of the Centre for the Law and Economics of Cyber Security at Erasmus University Rotterdam. His research focuses on data breach notification laws, cyber insurance and efficient investments in cyber security.

Prof. dr. Michel van Eeten's chair at TU-Delft focuses on the Governance of Cybersecurity. He studies the interplay between technological design and economic incentives in Internet security.

Prof. dr. Michael Faure is professor of law and economics at the universities of Rotterdam and Maastricht and is haiwaimingshi (distinguished foreign professor) at the Centre for Law and Economics of the China University of Political Science and Law. His core research is focused on the law and economics of systemic risks.

We are grateful to the members of the subcommittee and secretary of the Dutch Cyber Security Council for their valuable feedback, support and useful comments on an earlier version of this report. Also, we thank the experts that have been interviewed for their time and input. Last, we thank Florence Arke for her research assistance.

Table of Contents

List of Abbreviations

AVG	Algemene verordening gegevensbescherming (The Dutch GDPR)
DBNO	data breach notification obligation
E.U.	European Union
GDPR	The EU General Data Protection Regulation
NIS-Directive	Directive on security of network and information systems
U.S.	United States
WBNI	Wet beveiliging netwerk- en informatiesystemen (NIS-Directive)
WGMC	Wet gegevensverwerking en meldplicht cybersecurity (Dutch security breach notification obligation)
WOB	Wet Openbaarheid van Bestuur (Dutch Freedom of Information Act)

Executive summary

One of the most significant issues in cyber security is the lack of information diffusion about the nature of cyber risk and the return on investment of strategies that aim to reduce it. This study investigates one possible method to increase cyber security information diffusion: the extended public disclosure of data breaches that already are notified according to the data breach notification obligation in the GDPR. The study uses a literature review, expert interviews, feedback from the CSR data breach notification obligation subcommittee and written feedback rounds.

We studied the current form of public disclosure of data breaches, the legality of extended public disclosure and the costs and benefits thereof. One of the benefits is the learning effect. The general logic is that more public information about the data breaches provides society with the opportunity to learn more about the nature of data breaches, trends and the return on investment of cyber security investments. Next, we drew several building blocks of a public disclosure regime and came up with five alternatives:

1. **The Benchmark alternative** constructed as follows:
    a. Which segment? Public disclosure of the data breach data related to both Article 33 and Article 34 GDPR.
    b. Which information? Data on an individual data breach level, such as the name of the data controller, the amount of records, the type of data breach, the causes of the breach and the measures taken. This is the information provided in Appendix A, with the exception of the contact details of the individual within the organization that provided the notification.
    c. When? Public disclosure directly after the breach.
    d. To whom and how? Public disclosure to the general public in a central register.
2. **Delayed public disclosure** deviates from the benchmark alternative by disclosing data breaches after one year instead of immediately after the breach. Hence the public data breach register will be supplemented with a delay of, for example, one year.
3. **Full delayed disclosure with selected parties.** In this alternative, only selected parties would get the data breach data after a certain period that has to be determined by the DPA. In practice, research institutions, crime departments and CERT communities could apply for the data at the DPA. The latter should constitute a central point of contact for this procedure.
4. **Pseudonymized open access extended public disclosure** is a fourth alternative for extended public disclosure. It entails open access of data breaches, but without naming the organization that notified.
5. **No extended public disclosure.** One could also opt for no further public disclosure of data breaches, in combination with research that assesses alternative methods that aim to achieve similar goals of stimulating information diffusion in cyber security. In that case, the status quo of the data breach notification regime remains.

In short, we can conclude that extended public disclosure is good for society but has net costs for the organization that notifies. However, private costs are largely perceived reputation damage. This points out at a crucial role of the positioning of extended public disclosure. In the context of the 'risk free society', data breach disclosure should not be viewed as a bad thing, but as something society can learn from. If not, there is a risk that the perceived reputational damage related to extended disclosure can reduce the willingness to notify.

1. Introduction

Cyber security incidents occur on a daily basis and will continue to occur in the future. Government, industry and individuals must keep up. Their cyber security investment strategy regarding these incidents determines the eventual organizational and societal cost of cyber security. But how do we know what are efficient and effective means to invest in cyber security to keep our organizations secure at acceptable social cost?

One of the most significant issues in cyber security is the lack of information diffusion about the nature of cyber risk and the return on investment of strategies that aim to reduce it.[1] This is caused by the fact that information regarding the nature of cyber risks and the return on investment of cyber security investments is distributed asymmetrically among actors. Often, actors solely have access to their own loss data and cyber security investment data, which is insufficient to generate a complete picture of the costs and benefits of cyber security investments and trends in cyber security. In order to increase social welfare, this data should be diffused and aggregated. This study investigates one possible method to increase cyber security information diffusion: the extended public disclosure of data breaches that already are notified according to the data breach notification obligation in the GDPR.

This introduction will first briefly introduce the data breach notification obligation in the GDPR. Secondly, we will discuss the scope and goal of this research and finally our methodology.

1.1. The GDPR

The GDPR is here. Since the 25th of May 2018, the European Union has one of the, if not the, most extensive and fierce privacy regimes in the world.

The GDPR regulates many aspects related to the processing of personal data such as basic principles (Article 5), lawfulness of processing and individual consent (Article 6) and rights of individuals that have provided their data to a third party (section 2 of the GDPR). The GDPR entered into force on May 24, 2016 and applies after a two-year transition period from May 25, 2018.[2] Contrary to its predecessor, Directive 95/46/EC,[3] the GDPR will equally apply directly to every citizen and organization falling within the scope of European Union law.[4]

The GDPR contains a data breach notification obligation (DBNO), incorporated in Articles 33 and 34. The EU DBNO imposes an obligation on organizations to disclose certain breaches of personal data to a notification authority and to affected individuals (hereafter: data subjects).

The GDPR, and therein the DBNO, has a large impact on both government and industry. The Data Protection Authority has received thousands of data breaches. In fact, in the Netherlands, there have been more data breach notifications in one single year than in the whole of the U.S. over an eight years period.[5] Hence, the DBNO is generating an enormous amount of data.

One should however be aware that the social effects of the DBNO strongly depend on whether the data that has been generated will be disclosed in public or will kept secret.[6] If by the end of the day notifications would merely end up in a digital

1. Nieuwesteeg (2018).
2. GDPR, Art. 99.
3. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).
4. Directive 95/46/EC (Data Protection Directive) did not contain a requirement to notify data breaches.
5. The Dutch national predecessor of the EU DBNO in the GPDR. This national law that was adopted in anticipation of the GDPR. For example, in 2017, the Netherlands encountered 10009 data breaches in the year 2017 (https://autoriteitpersoonsgegevens.nl/nl/nieuws/10000-datalekken-gemeld-2017) while there are 8681 U.S. data breaches collected between 2006 and 2018 by the website privacyrightsclearinghouse.org (27 august 2018).
6. See the analysis in Chapter 4 based on the available scientific literature. Some parts of the analysis in this scientific report are based on earlier scientific publications of the authors, namely Nieuwesteeg (2018) and Nieuwesteeg & Faure (2018). In a some instances, the text of this report can be identical to the text used in these publications.

drawer at the DPA and no further action is taken to promote cyber security, then possibly the entire DBNO would only be an extremely costly exercise with relatively little social benefits as far as improving cyber security is concerned. This points at the crucial role to be played by the analysis in this report on the costs and benefits of public disclosure to make the DBNO a success.

Currently, data breaches are only limitedly disclosed publicly by the DPA and on an aggregate level. This report will take a deep-dive into one possible solution in enhancing the effectiveness of the DBNO, namely to publicly disclose data breaches by the DPA. The goal of this report is to identify the potential added value as well as the possible adverse effects of public disclosure. The endeavor of this report is accumulated in the following research question:

What are the effects, legality and alternatives of extended public disclosure of data breaches?

1.2. Scope and goal of this report

This report will exclusively look into the possibility of extended disclosure of data breaches in order to enhance social welfare in cyber security. We consider the mechanism welfare enhancing if the social costs (the sum of the individual private costs of citizens and organizations in society) are lower than the social benefits thereof. In simple words: to make society more cyber secure at acceptable cost.

This paradigm resembles our definition of 'effectiveness': a contribution to social welfare, for instance the right to know of individuals, learning about cyber security and the sunlight of disinfectant principle. Those social benefits (and the costs thereof) are extensively discussed in Chapter 4.

We will not look into alternative legal instruments or mechanisms that are also capable of enhancing social welfare related to cyber security. Within the possibility of discussing extended public disclosure, we will discuss several alternatives, which are discussed in Chapter 5. Other mechanisms or legal instruments that are capable of solving issues in cyber security are discussed in the concluding Chapter in the section 'avenues for future research'.

Furthermore, it is important to note that this report is an analysis of the costs and benefits of extended public data breach disclosure. It is not an advice for a certain policy.

1.3. Methodology

The study uses a literature review, expert interviews, feedback from the CSR data breach notification obligation subcommittee and written feedback rounds.

Literature review. Based on the available scientific literature, we analyzed the effect of public reporting of data breaches within the frameworks and possibilities of the data breach notification obligation in the GDPR. An overview of the scientific literature that has been used in the context of this report is included in the reference list.

Expert interviews. We interviewed experts from both university, government and industry on this topic. Experts should have either knowledge of the technical legal system of data breach disclosure or knowledge about the private and social costs and benefits of data breach disclosure. The list of interviewees is displayed at the end of the report.

The following questions are addressed: What are the benefits of public disclosure of data breaches? What would public disclosure cost? Who should decide on disclosure of data breaches? What information should be shared? When should information be made public? To whom should information be made public? In what way would information be made public?

The interview data is used to qualitatively strengthen the analysis by real world experiences of the interviewees, such as the public disclosure of the Fox-IT data breach, to gain insights about the legal aspects of public disclosure, to illustrate arguments related to costs and benefits and to assist in the identification of the desirability of the choices made in the building blocks that lead to the alternatives of public disclosure.

Feedback from CSR data breach notification obligation subcommittee. The feedback from the CSR subcommittee is primarily used to further constructing and scrutinize alternatives for public disclosure based on the available building blocks and gathering information about the possible impact these alternatives will have.

2. Current forms of public disclosure of data breaches

In order to evaluate what could be improved, we need to first understand how data breach notification and public disclosure currently works. In the EU, these regimes have been introduced quite recently. As such, there is only limited research available on their effects. We therefore also explore the situation in the U.S., where mandatory data breach notification has been in existence for over a decade. Furthermore, many of the U.S. state laws include broader forms of public disclosure of the notifications than the current practice in the Netherlands. A range of studies is available that has collected data in the U.S. on the effects of disclosure. These studies help us to evaluate the cost and benefits of extending public disclosure in the Netherlands.

Before we turn to the U.S. regimes, we first discuss data notification and public disclosure in the EU – most notably, the GDPR and via third-party data breach disclosure.

2.1. The notification system in the GDPR

The GDPR introduces public disclosure of data breaches by means of its data breach notification obligation (DBNO). The GDPR provides for the DBNO in Articles 2(2), 4(7), 4(12), 33, 34 and 83(4). There are two forms of public disclosure: public disclosure ex Article 33 and public disclosure ex Article 34, which we will discuss respectively. The following Articles define core building blocks of the current forms of public data breach disclosure in the GDPR, and are indispensable for a further analysis of public disclosure.

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

Article 4 (12) defines a personal 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'. The definition thus focuses on the consequences of the data breach. In doing so, the EU legislator incorporates the 'CIA triad' of confidentiality, integrity or availability of personal data.[7] Possible differences in the origin of the data breach, for instance whether a data breach is intentional or negligent, are not relevant for defining a data breach.

Articles 4 (7) states which entities have to notify data breaches. These 'data controllers' can be legal persons or public authorities. Hence, the DBNO applies to both public and private organizations.

Article 2 (2) excludes certain data breaches from the notification duty. Data that (a) falls outside the scope of EU law; (b) falls within the scope of Chapter 2 of Title V of the TEU; (c) is carried out by a natural person for personal use or (most notably) (d) is used for the execution of criminal prosecution do not have to be notified when breached.

Article 83(4) states that a sanction of €10,000,000 or 2% of the undertakings turnover, whichever is higher, can be imposed when the data controller fails to notify a data breach.[8] These sanctions are high compared to the sanctions in the U.S., whereby state level DBNOs usually have sanctions in the magnitude of $100,000s or lower.[9]

7. Pfleeger (1991).
8. GDPR, Art. 83(4); GDPR, Art. 83(2) specifies guidelines for the determination of the actual magnitude of the sanction.
9. For an analysis of the proposed legislation, see Nieuwesteeg (2014). Note that only a part of the data breaches necessarily have a relation with cyber security, because not all data breaches are digital. For instance, in 2017, 6% of the data breach notified were caused by hacking, malware or phishing. However, data breaches related to cyber security tend to have a larger impact because often more records are breached than cases where data is sent to a wrong recipient. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_2018-02-23_2017_jaarrapportage_algemeen.pdf.

2.2. Public disclosure through statistics of the DPA

As said, articles 33 and 34 regulate the actual obligation to disclose a data breach.[10] There is a difference in notifying a data breach to a data protection authority (DPA, Article 33) or to the data subjects affected (Article 34). This section will discuss public disclosure under Article 33 and the following section will discuss disclosure subject to Article 34.

Which information should be notified to the DPA? With respect to Article 33, a data controller has to notify the DPA 'unless the personal data breach is *unlikely* to result in a risk to the rights and freedoms of natural persons'.[11] Hence, this 'likelihood' is the key threshold for notifying the DPA. Article 33(1) further specifies that the notification should be as soon as possible, and not later than 72 hours after the data breach has been discovered. However, this is apparently not a red line, because if it is not feasible to do so, the organization can notify later, but has to specify the reasons why it does so. Under 33(3), the data controller has to include the nature of the breach, its consequences for data subjects, a description of counter-measures undertaken and a contact point. When possible, the organization should also include the type and number of affected data subjects and the amount of records, which have been breached. The practical implementation can be viewed on the websites of the various DPAs in the EU.[12] Appendix A displays the information that currently needs to be provided to the DPA. The categories of the notification system are as follows:

1. Contact data and other general information
2. Timeline
3. The nature of the data breach
4. Categories of personal data that have been breached
5. The group of people whose personal data are involved in the data breach
6. Measures that are taken before the data breach took place
7. Consequences of the data breach
8. Follow-up actions in response to the data breach
9. Additional information

Table 1: overview of data breach disclosure in the EU

Publicity trigger	Form of disclosure	Number of data breach notifications in the Netherlands
Article 33 GDPR	Aggregated statistics by the DPA: • Total number of breaches • Distribution per sector • Distribution per breach type	15863 (2016-2017)
Article 34 GDPR	Individually informed data subjects: • Nature of the breach • Consequences • Measures taken	7011 (2016-2017)
Third party discovery	Free format	Unknown, see for instance the blackbook of the Dutch Privacy Organization Bits of Freedom[a] or data breaches related to the website haveibeenpwned.com

[a] https://www.bof.nl/category/zwartboek-datalekken/

10. Of less importance for this paper it the obligation under Article 33 (2) which states that data processors, which process data on behalf of the controller, have the obligation to notify the controller without undue delay after becoming aware of a personal data breach.
11. As such, it is quite peculiar that the Article speaks of a likelihood *to result in* a risk, since risk also contains the element of likelihood. (risk = likelihood * impact). Hence, within this paper, we will just use the term risk.
12. For instance, see <https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?1> or <https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/> or <https://www.datainspektionen.se/globalassets/dokument/blankett-2-anmalan-av-personuppgiftsincident--eng.pdf>

What is the form of public disclosure? The DPAs use this information to provide statistics about the number of data breaches on a highly aggregated and anonymised level. For instance, the Dutch DPA has provided information regarding the total number of data breaches, the type of data breaches and the distribution of data breaches per sector, which can be viewed in the figure below.[13]

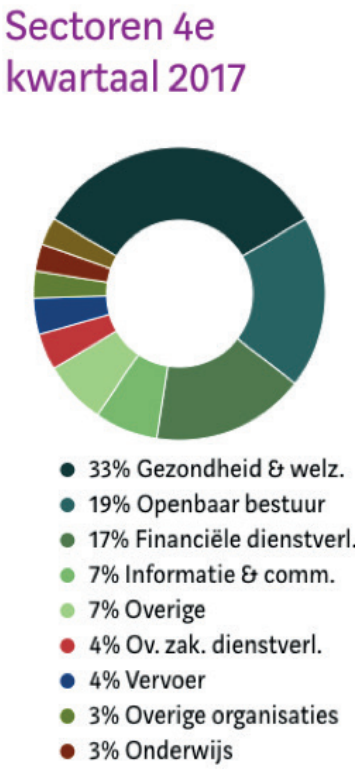

Figure 1: an example of aggregated public disclosure by the Dutch DPA

2.3. Public disclosure through informed data subjects

Article 34 regulates public disclosure through informing data subjects. Article 34 shows that the threshold for mandatory notification to data subjects is higher on several points compared to the requirements for notifying the DPA ex Article 33.

When should individuals be notified? First, notification to data subjects is only mandatory when the data breach is 'likely to result in a *high* risk to the rights and freedoms' of data subjects. Hence, where in Article 33 a certain risk suffices, in the case of Article 34 the risk should be high. The GDPR does not specify this gap between risk and high risk any further. The guidelines on Personal data breach notification under the GDPR provide some 'examples of personal data breaches and who to notify' in Annex B , but these examples are not clear since the very examples state that it depends on the circumstances of the case whether a data breach entails a risk or a high risk.[14]

Concerning the temporality of notification, Article 34(1) solely determines that this should be without undue delay and does not specify the 72 hours of Article 33. Article 34(3) provides three possible arguments that organizations can use not to communicate to data subjects. First, organizations may refrain from notifying data subjects when the data is made sufficiently difficult to use, for instance with encryption.[15] Second, when the organization has taken 'subsequent measures', which ensure that the high risk will no longer materialize, they do not need to notify. Third, notification to data subjects is not necessary when it would lay a disproportionate burden on the organization. Ergo, there is quite a large difference in the execution of notification to the DPA and to the data subject. The GDPR does not state the reasons for this difference. However, Article 34(4) regulates that the DPA may require the organization to still issue an additional notification to data subjects when the DPA assesses that the likelihood of adverse consequences for data subjects is 'high' according to Article 34(1).

What form of public disclosure? The exact information that should be transferred to the data subjects is specified in Article 34(2): 'The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data

13. See <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/cijfers-meldplicht-datalekken-vierde-kwartaal-2017>
14. Hert and Papakonstantinou (2016).
15. The topic of encryption and DBNOs, although not in the context of the GDPR, is extensively discussed by Burdon, Reid and Low (2010).

breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).'

The European Data Protection Board (EDPB), and its predecessor Working Party 29, contributes to the specification of the form of public disclosure. The EDPB is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union. Before the GDPR, the Working Party guidelines[16] already stated that the data controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

Furthermore, the working party specifies that 'Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual.[17]

2.4. Public disclosure through third parties

Apart from disclosing data breaches under the regime of the GDPR, also independent parties engage in disclosing data breaches. This could be disclosed by (either white hat or black hat-) hackers, black books by privacy organizations, crowdsourcing, media, people that gather or trade information on black markets or a combination of these actors. In theory, it is even possible to make much of the information disclosed ex Article 34 GDPR publicly available, when one crowdsources among the individuals that have been notified under the obligation of that Article. Quite naturally, the information that is made public varies from case to case since it is not subject to any regulation. Research in the U.S. has shown that not all data breaches are discovered by third parties, but still, these disclosures account for a significant amount of total data breach as can for instance be observed in the daily news reports about data breaches.[18] In that sense, public disclosure is already happening, but out of the span of control of the government.

2.5. Overview of public data breach disclosure in the EU

We can observe that there is a clear difference in notification ex Article 33 and Article 34. Slightly more than half of the data breaches which are notified to the DPA are not notified to the data subjects. These data breaches thus apparently do not result in a high risk into the rights and freedoms of individuals, according to the entity doing the notification. It is important to note that in both situations the information that reaches the public (either through aggregated statistics or individual notification by data subjects) is only a fraction of the information that data controllers provide to the DPA. (Compare the Appendix A, which summarizes all available data the DPA receives).

2.6. Public disclosure in the U.S.

The regulation of data breach disclosure traces back to the early 2000s. The U.S. DBNOs are regulated on a state level instead of the EU DBNO which is regulated at a central European level. California was the first U.S. state to adopt a DBNO in 2006 and other states quickly followed.[19] As of

16. Article 29 Data Protection Working Party: Guidelines on Personal data breach notification under Regulation 2016/679, p. 20.
17. Article 29 Data Protection Working Party: Guidelines on Personal data breach notification under Regulation 2016/679, p. 21.
18. Bisogni, Asghari, van Eeten (2017).
19. Nieuwesteeg (2014).

March 28, 2018, Alabama became the 50th and final state to enact a DBNO.[20]

Hence, the public disclosure of data breaches varies from state to state, but the general regime seems to be following an opposite order of notification approach. The European Union regulator first requires data controllers to notify the DPA. In more severe instances, it requires data controllers to notify the data subject. Hence the threshold for notifying the DPA is lower than notifying data subjects.

In the U.S., the situation is the other way around compared to Europe. U.S. data breach notification laws require, given a certain threshold, data controllers to notify data subjects. Only in some of the states, the law requires additional notification to the attorney general or consumer reporting agency.[21] Because the design of the DBNO varies (slightly) across U.S. states, so does the form of public disclosure. Hence, data breaches are not published on a national level. There are however, third parties, such as the Privacy Rights Clearinghouse, which collect data breaches that have been publicly disclosed in some form or another (for instance, by Attorney Generals, the media or notified data subjects). Only estimations have been made of the total number of data breaches per year. Bisogni et al., for instance, estimated 1264 breaches reached the Attorney General for the year 2015.

In the U.S., the administrative penalties for DBNOs are usually two orders of magnitude lower than in the EU DBNO. For instance, the Virginia data breach notification law, which has one of the highest sanctions in the U.S., allows for an imposition of a $150,000 fine.[22] However, in the U.S., privacy class actions could be a much more significant cost for organizations.[23] This could be a possible explanation for the lower amount of data breach notifications in the U.S.

Table 2: overview of data breach disclosure in the U.S.

Publicity trigger	Form of disclosure	Number of data breach notifications in the U.S.
Data breaches through customer reporting agency/ attorney general	From a sole notification obligation to individuals to notifying the Attorney General or Consumer Reporting Agency, varying by state	1264 in 2015 (estimation by Bisogni et al.) [a] (in the same period, 547 data breaches were discovered by the third party website privacy rights clearinghouse).
Third party discovery	Free format	8681 (between 2006 and 2018) [b]

[a] Bisogni, Asghari, van Eeten (2017).
[b] Third party collection by the website privacyrightsclearinghouse.org (27 august 2018). There are also other website (overlapping with the privacy rights clearinghouse), such as idtheftcenter.org and veriscommunity.net/vcdb.html. The privacy rights clearing-house is most used among scholars in the law and economics of cyber security.

20. Vold (2018).
21. And in the cases of Idaho and Illinois, the CIO of the Department of Administration and General Assembly, Bisogni, Asghari, van Eeten (2017), p.4.
22. Code of Virginia §18.2-186.6.
23. Romanosky, Hoffman and Acquisti (2014).

3. Is more comprehensive public disclosure allowed?

It is obvious that the forms of public disclosure in the sense of Articles 33 and 34 of the GDPR are legally allowed and even obligatory. Article 33 regulates disclosure to the DPA and Article 34 regulates public disclosure through informing data subjects. Think of the fact that notifications to data subjects make up around half of all breaches reported to the DPA. This means the breach is already disclosed, even though not all of them might reach a wider audience. This chapter discusses whether more comprehensive forms of public disclosure are legally feasible. Of course, extended public disclosure can be designed in many different ways. We will discuss this in Chapter 5 and 6. Here, we will explore legal feasibility and constraints of a reference model with a comprehensive public disclosure mechanism that resembles the situation in a number of the U.S. states and the data that is being notified according to the DBNO in the GDPR:

- Which segment? Public disclosure of the data breach data related to both Article 33 and Article 34 GDPR.
- Which information? Data on an individual data breach level, such as the name of the data controller, the amount of records, the type of data breach, the causes of the breach and the measures taken. This is the information provided in Appendix A, with the exception of the contact details of the individual within the organization that provided the notification.
- When? Public disclosure directly after the breach.
- To whom and how? Public disclosure to the general public in a central register.

We will call this reference model the *benchmark extended public disclosure.* This quest for the legality of the various alternatives under scrutiny in this report contains the assessment of three pieces of legislation. First, we will consider the possibilities for extended public disclosure in the GDPR. Secondly, we will investigate whether Freedom of Information Acts, more specifically the Dutch Freedom of Information Act 'Wet Openbaarheid van Bestuur' contains starting points for an analysis into the legality of extended public disclosure. Last, we discuss the NIS directive (Directive on security of network and information systems).

3.1. The GDPR

The GDPR does not mention the form of extended public disclosure of data breaches as subject of this research, which goes beyond the public disclosure in Article 33 and Article 34. Hence, this means that there are no explicit prohibitions of extended public disclosure. On the contrary, there are positive provisions in the GDPR that provide member states the discretionary freedom to give the DPA other powers and responsibilities.

Article 58 (3)(b) states that the DPA has the power to 'to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data'. Some of the experts consulted have indicated that this Article is the basis for providing the aggregated data reports that were mentioned in the context of discussing the form of publicity flowing from the obligations in Article 33 (notification to the DPA).[24]

In addition, ***Article 58 (6)*** states that 'each Member State may provide by law that its supervisory authority shall have additional powers.' Hence, this is a relatively broad Article that gives member states the possibility to extend the office of the DPA, for instance with powers that solely concern national matters. The Article furthermore states that 'The exercise of those powers shall not impair the effective operation of Chapter VII of the regulation', which entails amongst others the consistent application of the GDPR between DPAs in the European Union.

Chapter VII of the regulation describes the measures to ensure a consistent application of the regulation. One of the measures is a consistency mechanism, that provides for procedures to keep

24. CIOPN (CIO Platform Nederland) has also supported the provision of more detailed but still aggregated information/analysis from notified breaches by the DPA.

consistency in the application of the GDPR. It becomes clear that there would be no positive obligation for DPAs to discuss possible extended public disclosure of data breaches through this consistency mechanism. The consistency mechanism mostly describes specific topics to agree upon. The extend public disclosure is not one of them, because this topic is not discussed at all in the GDPR. However, Article 64(2) states that 'Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion.' Article 65(1)(c) states that ultimately the board can adopt a binding decision when a DPA does not follow an opinion under Article 64(2). The opinion has to have a two third majority (Article 65(2)).

On top of the consistency mechanism in the GDPR, one should be aware that the GDPR is a regulation. The 'regulation' is the strictest legal instrument in EU law. The GDPR aims to harmonize activities regarding data protection that fall under the scope of the regulation in the EU. Hence, apart from the specified consistency mechanism, there is a broader obligation under EU law (and in the GDPR) to consistently apply the GDPR in every member state. Thus, the question in this respect is not whether the GDPR prevents extended public disclosure, but whether the consistency argument prevents a single DPA from additionally disclosing data breaches, and whether such a measure must be unilaterally implemented throughout the EU.

In order to investigate this issue, we would have to identify whether the additional activities of the DPA, namely to implement a more far reaching form of public disclosure, have an impact on the operation of the activities that fall within the scope of the GDPR.

This could for instance be the case when extended disclosure would be interpreted as an additional punishment for the organizations that notify data breaches. Such an additional punishment would be not consistent with the operation of the GDPR in other member states, because in other member states such a 'punishment' would not exist. In assessing this, we have to identify the change in private benefits and costs of disclosure, after the extended public disclosure, which we will do in Chapter 4.

All in all, there is no explicit prohibition of extended public disclosure. The GPDR even provides for some discretionary freedom of the member states to give DPAs additional duties and powers, insofar the consistency of the application of the GDPR is not impeded. Hence, this would be a main parameter for evaluating the alternatives in Chapter 6.

3.2. Freedom of Information Acts – the Dutch freedom of information act (WOB)

Freedom of Information Acts allow access by the general public to data held by governments. The DPA is a body of government. Hence, the data that has been notified to the DPA could be subject to the rights and restrictions under the various Freedom of Information Acts in the EU. Within the scope of this report, we will solely scrutinize Freedom of Information Act (WOB) in the Netherlands. The most relevant Articles for this discussion are Article 8 and Article 10.

Article 8. With regards to the Dutch WOB, we must first constitute that the governments in itself has a duty to autonomously provide information insofar this contributes to a proper 'democratic governance', which arguably can imply a broad range of information since no further specification is being made on which kind of information should be provided. In general, it is believed that more informed citizens can contribute better to a democratic society.[25] This Article can thus form an additional basis for providing information regarding data breaches. The information flowing from Article 8 is a decision according to the definition of the Dutch general administrative

25. See also Article 110 of the Dutch Constitution, which states: "In the exercise of their duties government bodies shall observe the right of public access to information in accordance with rules to be prescribed by Act of Parliament."

act.[26] This means that stakeholders (in Dutch law: 'belanghebbenden') with regards to the information that ought to be disclosed, should be asked for their opinion before disclosing the data.

Article 10, however, specifies the restrictions upon the disclosure of information, which could be relevant in the case of extended public disclosure of personal data breaches and also apply to independent disclosure of government agencies. Also the stakeholders that ought to be consulted can invoke the grounds in Article 10 for withholding the disclosure. This administrative process increases the societal costs of disclosure.

Article 10(1)(c) specifies that company data that has been notified to the government in confidentiality should be excluded from publication. It is important to note that this data concerns business confidentiality that gives a clear competitive advantage to competitors. For instance information that gives an insight in the production process of an organization.[27] It becomes clear that in most cases, data related to data breaches does not give a competitive advantage, because most organizations do not compete on cyber security. On the contrary: there are many initiatives whereby organizations that compete with each other (for instance banks or hospitals) share deep cyber security information (much deeper than the information provided to the DPA) with each other.[28] However, even if a judge would argue that the information would provide competitors with an advantage, the notification system in the GDPR in Articles 33 and 34 does not mention that the data breach data that has to be provided to the DPA should be treated confidential. It is important to note that we are not discussing 'personal data' in this respect, but solely data related to the incident which is not personal, such as the cause of the breach and the number of records that have been breached. The exclusion ground would arguably be further weakened when Article 34 breaches are taken into account since the data breaches are to a lesser degree confidential when they are notified to the data subjects, which are free to further distribute the data to the media and other sources.[29]

Article 10(1)(d) specifies that the disclosure of personal data is excluded from the Dutch freedom of information act. One should be aware that no actual personal data of the data subjects is being disclosed to the DPA under Article 33, only the number of records that has been breached. The data controller should however provide contact details of the individual that notified the data breach, which should be excluded from public disclosure according to this article.

Article 10(2)(g) specifies that when the public benefits of disclosure do not compensate for the private costs of the individuals or organizations involved, disclosure should be prevented. In Dutch legal practice, this exclusion ground has a high barrier, as it is a residual bucket when other more specific exclusion grounds fail. For instance, there are very few cases in which a judge prohibits disclosure on the basis of reputation damage.[30] The analysis in Chapter 4, which discusses changes in private and public optima after the introduction of extended public disclosure, will shed a light on this matter, and will show that U.S. research shows that there is no long term reputational effect that can be observed. Even when reputation damage would in itself be a ground, it is important for this argument to succeed in court that one organization should gain a disproportionate advantage or disadvantage following the disclosure. Since a data breach disclosure obligation applies uniformly towards all data controllers ex ante in the Netherlands, this would arguably not be the case. Of course, we should note that this is a broad exclusion ground, and we cannot discuss all possible lines of argumentation that could lead to a legal decision

26. Een Besluit in de zin van de Awb; interview met Cornelis van der Sluis.
27. Interview Cornelis van der Sluis.
28. For instance, under the regime of the NIS directive, but also in voluntary ISACs.
29. Which occurs very frequently in the US.
30. Interview with Cornelis van der Sluis.

that prohibits extended public disclosure.[31] For this to investigate further, it would be preferable to actually request the data breach data and provoke a legal decision.

3.3. NIS-Directive (Wet Beveiliging Netwerk en Informatiesystemen)

The Directive on security of network and information systems ('NIS' Directive 2016/1148) regulates cyber security for network and information systems, which are 'essential services' such as the energy and utility industry and key digital service providers such as search engines and online market places. Article 14 (3) regulates the security breach notification. Operators of essential services should, without undue delay, notify incidents having a significant impact on the continuity of the essential services they provide to a competent authority.[32] These incidents, such as for instance a cyber attack on a power grid, could also entail personal data breaches. These companies should however disclose personal data breaches under the GDPR regime.

In the Netherlands, the Directive has been transposed into national regulation by a law called 'Wet beveiliging netwerk- en informatiesystemen', hereafter Wbni. By implementing the NIS Directive, the Dutch legislator has chosen to ensure that, in general, the breach notification will be treated confidential by the Dutch competent authorities.[33] The question is whether this confidentiality requirement conflicts with various alternatives for extended public disclosure which are subject of this research and are discussed in Chapter 5 and 6.

It is relevant to observe that confidentiality in the context of business confidentiality is mentioned in Recital 33 and 41, Article 1(5) and Article 14(5). The first part of Article 14(5) states that 'On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.'

One should be aware that a potential conflict solely arises for the subset of organizations that fall within the scope of the Directive: operators of essential services and digital service providers. These parties should notify security breaches that have substantial impact on the continuation of their services. These security breaches are very rare. In the first year of the security breach notification (which was already adopted beforehand), the Dutch National Cyber Security Centre did not receive any compulsory notification in over a year time, although it received some voluntary notifications.[34] While at the same time, the Dutch DPA received 10.000 data breach notifications. Furthermore, those security breaches do not necessarily entail personal data and thus are not always notified to the Dutch DPA as well. Last, when such a security breach would contain personal data, the data is likely (given the high threshold of the security breach) to have a high impact on the rights and

31. For instance, one could argue that a disproportionate disadvantage would exist between organisations that notified in the Netherlands and the EU (which we already discussed in the context of the GDPR, when disclosure would be seen as an additional punishment), but on the other hand there are many cases (for instance related to food quality data) in which the Netherlands legally unilaterally discloses data of organisations.
32. Which is a different authority than the data protection authority of the GDPR, namely the NCSC and/or the specific supervisory authority for this organization.
33. The Dutch government already largely implemented a security breach notification obligation (Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) that fulfills the requirements of the security breach notification obligation in the NIS Directive and hence forms part of the new Wbni that transposes the EU directive.
34. In the first year of the security breach notification (which was already adopted beforehand), the Dutch National Cyber Security Centre did not receive any compulsory notification, over a specified threshold, in over a year time, although as was the case in previous years it received a substantial amount of voluntary notifications, see https://www.ncsc.nl/actueel/Cybersecurity-beeld+Nederland; one should be aware that the GDPR applies to every organization and the Wbni only to a (small) subset of Dutch organizations.

freedoms of individuals and therefore should be notified to the affected individuals anyway, which is at least some form of publicity.

To conclude, theoretically, the NIS directive could conflict with extended public disclosure of personal data breaches. However, there are a number of factors that reduce the urgency of this conflict between the breach obligations in the NIS Directive and the GDPR:

1. There is an extremely low number of security breaches that are notified under the Wbni regime.
2. Only a part of these security breach notifications will contain personal data
3. When a part of this already low number of breaches will contain personal data, public disclosure to affected individuals occurs anyway when it has a high impact on these individuals, which is likely given the high threshold for the NIS Directive.

3.4. Conclusion

The conclusion of this chapter is that the legality of extended public disclosure strongly depends on the chosen alternative. First, the EU consistency mechanism, and the broader harmonization goal of European policy dictates that a form of extended disclosure that significantly alters the operation of the GDPR will at the least require a consistent application throughout the EU. For instance, extended disclosure could be seen as a significant alteration to the operation of the GDPR when extended disclosure is being seen as an additional punishment for data controllers. Secondly, it becomes clear that a form of extended disclosure that involves any personal data of the point of contact that disclosed, will not be allowed by the Dutch Freedom of Information Act. And thirdly, according to the same Freedom of Information Act, the public benefits of disclosure must clearly exceed the private costs of disclosure and there must not be disproportionate advantage or disadvantage of a single party.

Hence, extended public disclosure would be allowed as long as the extended public disclosure a.) would not be seen as an additional punishment, b.) would not include personal data of either the individual that functions as a contact point for the DPA or personal data related of the data subjects that were affected by the breach and c.) would not disproportionately affect some of the organizations that notified.

It becomes clear that the reference model could sustain when the extended form of public disclosure cannot be seen as an additional punishment and extended disclosure would apply unilaterally over all data controllers that notified the DPA. However, the Dutch Freedom of Information Act would arguably increase the costs of some variants of extended public disclosure, since stakeholders must be asked for their opinion in the process.

4. What are the costs and benefits of public disclosure?

This section discusses the costs and benefits of extended form of public disclosure by using the reference model we introduced in the previous section, the *benchmark extended public disclosure*. It entails:

- Which segment? Public disclosure of the data breach data related to both Article 33 and Article 34 GDPR.
- Which information? Data on an individual data breach level, such as the name of the data controller, the amount of records, the type of data breach, the causes of the breach and the measures taken. This is the information provided in Appendix A, with the exception of the contact details of the individual within the organization that provided the notification.
- When? Public disclosure directly after the breach.
- To whom and how? Public disclosure to the general public in a central register.

Remember, this model resembles the notification and disclosure laws in certain U.S. States and the information that is being notified to the DPA by the data controller according to the current notification regime in the GDPR ex Article 33. Before we turn to exploring the costs and benefits of the reference model, we survey the leading empirical studies on the costs and benefits that have occurred in practice in the U.S. This will give us a basis of evidence, albeit partially, from which to conduct our evaluation of the effects and costs and benefits we could expect in the Netherlands.

First, we will discuss the private costs and benefits for the organization that notifies the data breach. Second, we will discuss costs and benefits for society. We will discuss the *change* in private and public optima after the introduction of extended public disclosure.

This discussion is important for various reasons. First, as we discussed in Chapter 3, the legality of public disclosure could depend on the change in the burden of the organization that notified (the 'private cost' of disclosure). This is both relevant for the GDPR (because these extra private costs could be seen as additional penalties) and for the Dutch Freedom of Information Act, which forbids disproportionate disadvantage. Furthermore, the legality also depends on the public benefits of the law, because the Freedom of Information Act demands that public benefits costs must outweigh private costs.

Second, the discussion of private and public optima (the sum of costs and benefits) yields valuable insights into the eventual design of the various ways in which extended public disclosure could be implemented. The reference models helps us to understand the *direction* of the *change* in private and public benefits when extended public disclosure would be adopted. For instance, data controllers may already incur communication costs when disclosing data breaches to their customers. These communication costs may rise when these breaches are disclosed in a central register, because privacy organizations, the media and consumer associations might ask additional questions. Hence, we will discuss the change in communication costs.

When constructing and comparing different alternatives, the *direction* of this change will stay the same, although the intensity of the effects will differ amongst the chosen alternatives.

4.1. Research in the U.S.

This section briefly summarizes key research that analyses the effectiveness and effects of data breach disclosure and data breach notification laws in the U.S. Section 2.6 pointed out, public data breach disclosure in the U.S. differs from data breach disclosure in the EU. Hence, the insights of U.S. research should not be transplanted directly to the other side of the Atlantic, but instead form useful building blocks for an integrated assessment of the effects of extended public disclosure, which is the subject of this study. The differences between the EU and U.S. situation is described further in Section 4.2.

The first (large) stream of literature covers reputation damage. The literature shows that data breach disclosure does have single digit (1 or 2%) negative market value impact on the short term. Reputation damage is usually quantified as the difference in company value before and after the disclosure. Goel and Hawsky (2009), used such an event study methodology. They measured the market value of the company a

few days before and after the notion of a security breach and found a negative effect of on average about 1% of the market value. Cavusoglu, Mishra and Raghunathan (2004) identified through a similar approach an incidental loss of stock prices of 2.1%. They discuss direct and indirect costs of data breaches, but this is a slightly different topic, as this paper is about to talk about data breach disclosure. Rosati et al. (2017) find that market activity on the short term becomes slightly higher after a data breach announcement. Ko and Dorantes (2006) used a matched sample comparison analysis instead of an event study methodology to investigate the impact of security breaches on firm performance. Their results are mixed. Overall performance of an organization that has been breached is lower (relative to organizations that incurred no breach), but sales increased. These observations about long-term impact should be taken with care, because the effect of the data breach is much harder to disentangle from other exogenous variables and high quality panel data is not available. Layton and Watters (2014) also indicate that firms can still grow, while writing-off some expenditures related to reputation damage. A survey by Ablon, Heaton, Laverey and Romanosky (2016) indicated that 11 percent of consumers indicated that they would stop dealing with the company following a breach.[35] Two Articles by Bisogni and Nieuwesteeg summarize the state of the art of scientific research towards reputation damage.[36] The overall pattern arises that data breaches could have some reputation damage on the short term, while effects on the long term are hard to disentangle from other exogeneous variables such as the growing demand for E-commerce. Market observations supports that huge data breaches do not prevent stock prices of companies to surge. Journalists at Bloomberg and Forbes observed that T.J. Maxx, JP Morgan or Adobe Systems all saw significant rises of their share prices after massive data breaches.[37] For instance, T.J. Maxx, had a data breach affecting 94 million customers in 2007. Their share price has risen from 15 USD in 2007 towards around 112 USD in October 2018.[38]

The second stream of literature covers the effectiveness of data breach notification laws by tying data breaches data to the desired policy outcomes. The most seminal paper in this respect is by Romanosky, Telang and Acquisti (2011), which discussed whether DBNOs reduce identity theft. They used panel data from the U.S. Federal Trade Commission to estimate the impact of data breach disclosure laws on identity theft from 2002 to 2009. Their conclusion: the adoption of data breach disclosure laws reduce identity theft caused by data breaches by, on average, 6.1 percent. Interestingly enough, the researchers invoked the Freedom of Information Act in the U.S. to get data on a lower aggregation level. Romanosky also studied liability and class actions related to data breaches together with Hoffman and Acquisti (2014). Their results suggest that the odds of a firm being sued are 3.5 times greater when individuals suffer financial harm, but 6 times lower when the organization provides free credit monitoring. This indicates that the damage an organization incurs following a data breach depends on the consumer response it offers. Also Nieuwesteeg (2014) measured effects of for instance penalties on the amount of notifications being generated by data breach notification laws. Related research covers the quantification or modelling of economic effects of DBNOs, such as Lenard and Rubin (2006) and Laube and Böhme (2016). The latter uses a theoretical model and also involves EU law.

The third stream of literature covers the topic of encryption and notification of data breaches in healthcare. Miller and Tucker (2011) identified that there is no empirical evidence of a decrease in publicized instances of data loss associated

35. Lillian, Heaton, Lavery and Romanosky, (2016).
36. Bisogni, Asghari and van Eeten (2017), Nieuwesteeg and Faure (2018). This report follows in parts of Chapter 2 and Chapter 4 the structure of the latter publication, which is written by (partly) the same authors as this publication. Hence, some phases of these parts of our analysis might show similarities with Nieuwesteeg and Faure (2018).
37. See <https://www.bloomberg.com/news/articles/2014-05-23/investors-couldnt-care-less-about-data-breaches> ; <https://www.forbes.com/sites/quickerbettertech/2014/06/02/why-did-t-j-maxxs-share-price-surge-after-a-data-breach-that-affected-94-million-customers/#77fbbea232a1>.
38. As of 17 October 2018.

with the use of encryption. Instead, they observe increases in the cases of publicized data breaches. Their argument is that data breaches do not result in a significant risk for the affected individuals anymore, and possible perceived reputation damage, and hence there is an increased incentive to publicly disclose the breach incident. Kwon and Johnson (2014) observe that data breach disclosure in healthcare can reduce data breaches on the long term. Kwon and Johnson (2015) study the market effect of data breaches in healthcare. They observe that data breaches do not affect patients' short-term choices but the cumulative effect of breach events over a three-year period significantly decreases the number of outpatient visits and admissions. However, Choi and Johnson (2017) show that data breaches in fact can lead to an increased 30-day mortality rate, possibly because of operational disruptions. The topic of encryption and DBNOs, although not in the context of the healthcare, is extensively discussed by Burdon, Reid and Low (2010).

A last stream of literature analyses the functioning of data breaches in the U.S. through interviews with security officers within companies and other stakeholders. For instance Schwartz and Janger (2007) and Mulligan (2007). Various other aspects of U.S. data breach notification laws have been researched, such as the timing of the notification studied by Bisogni (2015)[39], and, also by Bisogni (2016) the desirability of a federal law.[40] These last two aspects fall outside the scope of this report.

4.2. Differences between the EU and US

There are significant differences between the DBNO regimes in the EU and US. In this section, we will discuss the differences and where and whether they impact relevance of the insights of the scientific research in the U.S..[41]

A first difference lies in the set-up of the DBNOs. The EU DBNO is regulated at a central European level instead of at the state level for U.S. laws, which are partly much older than the EU law.[42] California was the first U.S. state to adopt a DBNO in 2006 and other states have followed in the past years.[43] Alabama became the 50th and final state to enact a DBNO as of March 28 2018.[44]

Secondly, there are also some notable differences with regards to the sanctioning regime, which is one of the corner stones for our scientific analysis,. In the U.S., the administrative penalties for DBNOs are usually two orders of magnitude lower than in the EU DBNO. For instance, the Virginia data breach notification law, which has one of the highest sanctions in the U.S., allows for an imposition of a $150,000 fine.[45] However, in the U.S., privacy class actions could be a much more significant cost for organizations.[46] One should however be aware that a fine or a class action is different from reputation damage, because these are real out of pocket costs of an organization.

Thirdly, more generally there are cultural differences between the U.S. and the EU in terms of for instance:

- Attitude to comply with regulation,
- Consumer attitude towards data breaches,
- Attitude towards public disclosure of data breaches

It would be quite ignorant to ignore these differences between the cultures of countries. Differences between people and attitudes are always an issue when performing empirical research. For instance, there are already huge differences within the U.S. which are possibly even larger than the differences between the U.S. and EU. Still, peer reviewed academic research focused on the legal developments and cyber security in a European Union context widely uses scientific insights from the vast number of data

39. Bisogni (2015).
40. Bisogni (2016).
41. See Nieuwesteeg & Faure (2018) for a more extensive analysis. This summary partly transposes the analysis in this publication.
42. Nieuwesteeg (2014).
43. Nieuwesteeg (2014).
44. Vold (2018).
45. Code of Virginia §18.2-186.6.
46. Romanosky, Hoffman and Acquisti, (2014).

breach that have been notified.[47] Unfortunately, there is limited research on the direction of these differences in the context of empirical research in the field of data breaches, precisely because of the lack of empirical data in the EU, which makes it unclear to point out the direction of the effect of these cultural difference. For instance, the question 'would a data breach in the Netherlands lead on average to lower or higher reputation damage than in Texas?' has not been subject to any research. Apart from differences, there are also similarities between U.S. and EU security professionals. For instance, consider the following quote "Our head of IT Security (of a major telecom) told us once, 'we have one key metric: Don't show up in the Wall Street Journal for a security breach.'".[48] This quote arguably could be a statement of a CIOs or CISO in the Netherlands. Hence, we will take the peculiarities of the EU legal regime into account in order to facilitate transplantation of the lessons learned on the other side of the Atlantic related to the social and private benefits and costs of extended public disclosure.

4.3. Private benefits

When analyzing private benefits and costs, we refer to the benefits and costs for the organization that would notify and disclose a breach, not the benefits and costs of other organizations. The latter will be discussed in the section regarding social benefits and costs. In general, the literature regarding DBNOs tells us that private benefits of data breach notification as such seem to be indirect and uncertain, while private costs are more direct and certain.[49] We can observe a similar situation when discussing the change in effects when extended public disclosure would be adopted.

Positive effect on the mitigation of impact and awareness. Extended public disclosure can lead to an increase in information and knowledge sharing regarding the data breaches, which could benefit the organization that notified.[50] This is arguably especially true for larger breaches in the database of the GDPR, for instance those data breaches that result from a hack. For minor breaches which are not caused by a cyber security threat, such as sending a data breaches to the wrong recipient, there is even a risk of notification fatigue.[51] Because data breaches are public, it is easier for other organizations to provide assistance regarding the mitigation and organizations do not have to 'reinvent the wheel'. This reduces transaction costs and increases cybersecurity awareness within an organization.[52] However, the benefits of openness immediately after the breach should be weighed against the risk of still being vulnerable for additional cyberattacks when disclosing these data breaches. This vulnerability effect is likely to exist only shortly after the breach as it could be expected (and it is obliged in most cases) that an organization takes appropriate measures after the data breach that mitigate the vulnerability. Extended public disclosure after a certain period can possibly raise additional awareness and incentives for a fast and effective mitigation of the vulnerability, which is essentially a private benefit.

4.4. Private costs

Besides benefits, private parties also incur costs when disclosing data breaches.[53]

Increased communication costs. Data controllers incur communications costs when they have to provide additional communication to data subjects or third parties, such as the media. In case

47. See for instance in the context of data breaches Nieuwesteeg & Faure (2018) and Laube and Boehme (2015), in the context of cyber insurance and cyber risk sharing: Biener, Eling and Wirfs (2015) which use a general framework for cyber insurance using both US and EU literature.
48. See the following article on Schneier's (2009).
49. Lenard and Rubin (2006), Romanosky, Telang and Acquisti, (2011), Nieuwesteeg and Faure (2018).
50. Nieuwesteeg & Faure (2018).
51. Nieuwesteeg & Faure (2018).
52. Romanosky, Telang and Acquisiti (2011).
53. These private costs, and the necessity to balance these costs with the social benefits of DBNOs have been debated in the literature. For instance, Burdon, Lane and Von Nessen (2012) mention competing rationales, such as the 'dual conflict of effective consumer protections relating to identity theft threats and minimising corporate compliance costs.'

the data controller already notified individuals, as part of the Article 34 GDPR obligation which states that data controllers should notify individuals in case the data breach constitutes a high risk to the rights and freedoms of individuals, communication costs are expected not to increase, or only slightly, since the individuals are already notified. In case of a data breaches which is only notified to the DPA, publishing the breach in a public registry (as in the reference model) would potentially increase communication costs, since clients of the data controller might hear about it and contact the controller to request more information. This effect largely depends on whether and how clients would learn about the breach after it is published in the register.[54]

Actual reputation damage can work out two ways. Before constituting the impact on reputation damage of extended public disclosure, we must briefly discuss the impact of reputation damage caused by data breach disclosure as such, because in general, there is a public misperception regarding the severity of this damage.

Section 4.1. discussed the stream of literature on reputation damage. The overarching pattern is that the potential reputational loss resulting from a public disclosure has relatively limited impact on the market value of companies, on average 1 or 2% a few days after the breach. On the long term, no effect has been pointed out.

Still, a nuance should be made. In practice, the distribution of reputational costs has a large tail. Some organization will suffer no significant long-term reputation damage, while other companies might go bankrupt because of the disclosure of the data breach, although the authors are not aware of any organizations who did. The former group is likely to consist of organizations with a stable customer base that are able to exploit lock-in strategies and are too big to fail. Another argument is that, apparently, consumers do not care about data breaches sufficiently, as for instance the data breach at Target shows, which apparently did not significantly affect their customer base.[55] A data breach does not reduce the likelihood that consumers buy the product or services of these organizations. However, one should be aware that nowadays, still, organizations often have to spend several millions, but these are often communication or liability costs. Another area of attention is the position of SMEs, which are usually not subject of research related to reputation damage.[56]

So, how would extended public disclosure affect the reputation damage of data controllers? It can work out two ways, depending on the implementation of the regime. The first line of argument suggests that there is a negative impact on reputation. When more data breaches are made public, regarding type Article 33 GDPR, breaches, or receive additional publicity relative to the individual data subject notification ex Article 34 GDPR, this would create additional awareness regarding data breaches of this particular company. This awareness could have a negative impact, when the register is used as a 'shame list' by privacy organizations, consumer associations or the (local) media in order to indicate which data controllers have relatively more data breaches.[57]

However, following a second line of argument, the disclosure of data breaches can actually have a positive impact on reputation when framed differently by the data controller and the DPA. This is particularly the case when society perceives data breaches not as related to bad security practices by the data controller but rather related to transparency and 'good citizenship' in relation to the disclosure of the breach. All in all, when an organization is honest and shows its vulnerability (and the measures taken) to its customers, this is a way to further connect with them. A transparent communication of the data breach could show that the data controller is able to deal with the breach in an effective manner without jeopardizing the interest of its customers. In that

54. See Section 2.1.2.
55. Nieuwesteeg (2018).
56. Interview with ms. Nicole Mallens and mr. David de Nood (VNO-NCW).
57. The experience in the US show however little evidence of a reputational effect. There might be some effect with regards to the medical sector. See the research by Johnson and Tucker described in the first section of this Chapter.

way disclosure could even reconfirm trust in an organization with an established reputation.

Fox IT, one of the leading IT security firms in the Netherlands, experienced a data breach and decided to go fully public. According to an interviewee in this organization, the decision to go public gained largely positive response of customers and other stakeholders.[58] In the end, perfect cyber security is not feasible, and even the best security firms will experience data breaches. The question is how to learn from your mistakes and to be transparent with it in order to share knowledge with other parties.

When data breach disclosure would be perceived as an act of transparency and contributing to the mutual learning system regarding cyber security, public disclosure could even have a positive effect. However, while the effect can be real, as showed in the Fox IT case, one should not be too wishful about the general application of this effect in practice. Still most organizations prefer (without any legislation demanding them to disclose) to conceal their vulnerabilities and data breaches, because they have strong perceived reputation damage.

Perceived reputation damage. In reality, reputation damage might be minimal or absent. Before disclosure, however, data controllers may *perceive* the threat of reputation damage after disclosing a data breach. As a security officer pointed out, "fear of reputation damage ... drives organizations to take steps to at least evaluate, if not correct and enhance security mechanisms."[59] Consider previously mentioned blog post: "Our head of IT Security (of a major telecom) told us once, 'we have one key metric: Don't show up in the Wall Street Journal for a security breach.'"[60] Probably, perceived reputation damage will only increase when the data controller become aware that every data breach will become publicly available. From the perspective of the data controller, this can feel like a 'slap in the face'.[61] Because reputation damage is solely an ex ante perceived costs, the only real result of it is the fact that data controllers will ceteris paribus disclose less data breaches when they perceive this effect as being real, which prohibits any social costs and benefits for society.

Liability / damages can increase. A fourth issue is liability. The general logic is that when a data breach become public, the opportunity arises for the public to sue organizations. Therefore, extended publication of data breaches raises the likelihood of liability costs.[62] However, when a company intentionally conceals data breaches and they nevertheless become public, it can reasonably be expected that the likelihood and impact of claims will be higher.

No additional administrative costs. First, there are the administrative costs of disclosing data breaches to the DPA. Administrative costs do not change when implementing extended public disclosure, when no further administrative actions of the data controller are required.

4.5. Social benefits

The literature labels several social benefits of data breach disclosure which could be amplified by extended public disclosure. In this section, we will discuss the right to know, consumer empowerment, information diffusion, the sunlight as disinfectant and liability.

Right to know. First, and foremost for the GDPR, the social benefit of data breach disclosure is the implementation of the data subjects' 'right to know' that their data has been compromised. This 'right to know' is an aspect of the fundamental right on the protection of personal data, enshrined in the Charter of Fundamental Rights of the European Union and the European Convention of

58. Interview mr. Erik de Jong (Fox IT).
59. Mulligan (2007).
60. See the following article on Bruce Schneier's blog: Schneier (2009).
61. Interview with ms. Lokke Moerel (Tilburg University).
62. See Nieuwesteeg and Faure (2018) for further discussion on this topic.

Human Rights.[63] The protection of personal data has been the primary reason for the European Union to adopt the GDPR and therein the EU DBNO.[64] The social benefit of the 'right to know' is intangible. Moreover, the value of the right to know will strongly depend upon the nature of the data breach. For example, it may be more important for an individual to be aware of an identity theft than of the loss of a username or password for a Steam account (a platform for mobile gaming).[65] How would this right to know be affected when there would be a form of extended disclosure?

Extended public disclosure could have a positive effect on the right to know in two ways. First, extended disclosure provides additional information ex ante, before the interaction with a data controller, when the information regarding data breaches would be transformed into a 'privacy list', for instance by third parties such as privacy organizations or consumer associations. The general logic is that consumers can have ex ante information about bad security practices at a certain organization they want to interact with on the bases of the data breach register, which could lead to consumer empowerment. However, it is questionable whether more data breaches in the notification system would imply bad security practices. Hence, one should be careful aiming at this effect, especially because it is strongly linked to (perceived) reputation damage of the data controller.

Secondly, extended disclosure provides additional information ex post, during or after the interaction with a data controller. When data controllers did make the decision not to notify individuals, but still notified the DPA ex Article 33, which they have done in roughly half the cases in the Netherlands, individuals can still identify whether the data controller they interact with, had a data breach through the public register. However, they cannot check whether they were personally involved because individual records will not be public.

Sunlight as disinfectant. The sunlight as disinfectant principle means that data breach notification drives the intensity of information security activities and awareness. When data breaches have to be notified (note that already the threat of notification has an effect), organizations want to avoid this by paying more attention to their security practices. This can lead to stronger incentives to mitigate the impact after the breach, and an overall improvement of cyber security on the long term. This has a number of trickle down effects. Because data breaches are more out in the open, this raises additional awareness among organizations regarding cyber security.[66] However, this should be balanced with the risk of notification fatigue when meaningless breaches are disclosed in the open.[67] Data breach disclosure has a short- term direct impact on mitigating and avoiding consumer[68] and organizational losses.[69] It also increases trust in security for consumers, because those who encountered in a data breach tend to be less afraid about cyberattacks.[70]

However, organizations and individuals may over-invest in their security improvements.[71] In the long term, according to U.S. chief security officers, data breach disclosure can foster "cooperation between information security departments".[72] This

63. Charter of Fundamental Rights of the European Union [2012] OJ C 326/1, Art. 8; European Convention of Human Rights, Art. 7. The right to know is described clearly in Article 8(2) of the Charter, which states that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".
64. GDPR, Art. 1.
65. This gradual decrease occurs independently of the absolute value of the right to know, which, as said, has to be determined by societal debate.
66. See for instance the research by Mulligan (2007).
67. Nieuwesteeg & Faure (2018); Nieuwesteeg (2018), <https://www.bernold.us/blog/opinie-artikel-in-fd-over-de-meldplicht-da-talekken>
68. Schwartz and Janger (2007) ; Mulligan (2007). This discussion is linked to the timing of the notification studied by Bisogni, (2015).
69. Romanosky, Telang and Acquisti (2011), p. 258.
70. Rainer Bohme, Marcus Riek Moore eurobarometer data ⟶ nog opzoeken
71. Lenard and Rubin (2006), p. 48.
72. Mulligan (2007), p. 18.

is also confirmed by Moore, Dynes and Chang (2015), who found that most firms indicated that cybersecurity was increasingly becoming a priority, either as a result of their own data breach experience or those of other firms. Having similar events clearly changed thinking in most firm's senior management about cyber-risk management. This diffusion of information has positive effects on overall security.[73] Furthermore, indirectly, data breach disclosure raises the public's awareness regarding cyber security. The question is to what extend this effect changes when there would be extended disclosure. Arguably, when there is more sunlight, the disinfectant effect would be stronger. However, eventually, when more less meaningful breaches would reach the public on top of the other breaches, for instance by a lower interpretation of the breach threshold, notification fatigue (see social costs), would eventually reduce this positive effect.[74]

Learning about cyber security. Apart from the apparent existence of the DBNO and the existence of data breaches flowing from the DBNO, which constitute the sunlight as disinfectant effect, there is also a learning effect regarding the data breaches as such. The general logic is that more public information about the data breaches provides society with the opportunity to learn more about the nature of data breaches, trends and the return on investment of cyber security investments.[75]

Arguably, extended public disclosure would greatly enhance the possibilities to learn from data breaches. The aggregated form of data (ex Article 33) or the individual notification of data subjects (ex Article 34) provide either little information or information which is not centrally available. U.S. research learns that the media can also not collect all information regarding data breaches.[76] Extended public disclosure can contribute to cyber security knowledge in a number of ways.

First, a register allows for enhanced scientific research regarding cyber security trends and threats. In the U.S., there has been much research on trends and threats by means of using 'flawed' data bases.[77] These data bases contain incomplete information regarding the total number of notified data breaches because not every data breaches has to be notified to the state level Attorney General or Customer Reporting Agency and only a part of these instances publicly disclose these data breaches. When the DPAs in the EU would opt for extended public disclosure of data breaches, this would result in a 'perfect database', in the sense that it contains all data breaches which are notified according the regime in the GPDR. This fully representative data base would greatly enhance the possibilities for research, even compared to the U.S. situation, which already has proven to be fruitful ground for learning from cyber security.

Second, extended public disclosure would foster research regarding the return of investment of cyber security measures.[78] Information related to cybersecurity trends and ROI of cyber security investments can lead to better products, such as cyber insurance. The cyber insurance market benefits from an increased availability of data because this allows for better premium determination.[79] As said, the change in the learning effect is high, because there are many additional breaches (and more information regarding each individual breach) flowing into

73. Ogut, Raghunathan and Menon (2005).
74. Nieuwesteeg and Faure (2018).
75. Nieuwesteeg (2018).
76. Bisogni, Asghari and van Eeten (2017) state that disclose data breaches from the attorney general have much more breaches in the dataset. Hence the media does not cover everything, but still some portion. Hence both significant portions of public disclosure come from DPA and from media. Hence, if DPA in EU would make things public than there will be significant increase of DBNs 'What is the insight?' 'And among the DBNL provisions, we see that attorney generals who publicly report notifications cause, on average, a 43% increase in reported breaches in that state. This effect was to be expected, though not perhaps its magnitude. More surprising is the fact that the requirement to report to credit agencies leads to a 34% increase, all other things being equal. Allowing the risk of harm exemption significantly decreases reports, by 21%.'
77. See for instance research by Edwards (2015), Nieuwesteeg (2014), Bisogni, Asghari and van Eeten (2017).
78. Nieuwesteeg (2018).
79. Nieuwesteeg (2018), Chapter 6.

the system with respect to media discovery, the scattered individual notification ex Article 34 and the aggregated data ex Article 34.

Liability. The potential liability claim that can follow a disclosure has a social benefit. Liability results in behaviour that incentivizes organizations to internalize some of the externalities in cyber security. Quite naturally, individuals can only claim damages when a data breach disclosure becomes public and they are aware of it. Hence, extended public disclosure has a positive effect on liability as a public benefit, but one should be aware the stronger the public benefit, the stronger also the private cost. Liability can even accumulate in class actions.[80]

4.6. Social costs

Additional communication costs on the consumer side. Arguably, when more breaches are out in the open through the extended public disclosure, consumers would face additional costs requesting information regarding these breaches, for instance whether they would be affected by it. Especially regarding Article 33 breaches, which should not impose a *high* risk on the rights and freedoms of individuals, there could be insufficient benefits for the consumer to compensate for these communication costs.

Additional notification fatigue. An increase in the amount of notifications can lead to a decrease in the positive effects of disclosure, because data subjects can pay less attention to each individual data breach. Subsequently, the information diffusion becomes less meaningful and eventually all data breaches could just be perceived as irrelevant information.[81] This effect is labelled as 'notification fatigue'.[82] This reduction of the 'sunlight as disinfectant' occurs at both an organizational level (which would possibly ignore the signalling function of data breaches as too many enter the public) and consumer level (which would be subjected to information overload which reduces their empowerment). It is important to note that notification fatigue does not only affect the benefits of the (least important) data breach, but also has negative externalities towards other data breaches. All data breaches become less important with the introduction of an additional data breach (through for instance extended public disclosure). Likewise, as soon as more notifications reach the public, the benefits of the additional data breach will decrease and the costs (the negative externality to other data breaches) will increase.

Reduction in trust in security and privacy. When more awareness regarding the hazards of the digital environment enter the public, this might lead to avoidance of digital services which would otherwise bring a net benefit to the party that uses them. An example is Internet banking fraud, which some believe reduces the likelihood of especially elderly people to us this service. Although a negative effect could not be ruled out entirely, the effect is likely to be small, because in general consumers tend to change from organizations when data breaches occur (see the reputation damage section).

Overreaction in restricting security. Organizations may over-, or inefficiently invest in security because of notifying the data breach and the threat that this data breach would be subject to extended disclosure. However, this is not expected to be a very significant social cost because in general, organizations have incentives to under-invest in cyber security.[83]

Reduction in willingness to notify. Extended public disclosure could reduce the willingness to notify according to the data breach notification regime in the GDPR when organizations perceive high reputation damage from extended public disclosure.

80. Especially in the U.S., see Romanosky, Hoffman and Acquisti (2011).
81. Mulligan (2007), p.33.
82. Nieuwesteeg and Faure (2018).
83. Due to the mainly positive externalities that are present in cyber security.

4.7. Overview

In this overview we display the private and social effects of extended disclosure. One should not that the estimations of the effects are made for the indicative purpose of the overview, and aim to reflect the insights of the literature. However, it is not a strict quantification of these effects.

Table 3: overview effects extended public disclosure

Effect	Change of effect after extended public disclosure
Private benefits	
Mitigation of impact	0/+
Private costs	
Reputation damage	0/-
Perceived reputation damage	- - -
Communication costs	-
Liability/damages	-
Administrative costs	0
Social benefits	
Right to know	+
Sunlight as disinfectant	+ +
Learning about cyber security	+ + +
Liability	+
Social costs	
Communication costs on the consumer side	-
Notification fatigue	- -
Overreaction in cyber security	0/-
Reduction of trust	0/-

5. Building blocks for a public disclosure regime

So far we discussed the private and social benefits and costs of extended public disclosure. In doing so, we took one point of reference, namely a *benchmark extended public disclosure alternative',* which entails:

- Which segment? Public disclosure of the data breach data related to both Article 33 and Article 34 GDPR.
- Which information? Data on an individual data breach level, such as the name of the data controller, the amount of records, the type of data breach, the causes of the breach and the measures taken. This is the information provided in Appendix A, with the exception of the contact details of the individual within the organization that provided the notification.
- When? Public disclosure directly after the breach.
- To whom and how? Public disclosure to the general public in a central register.

Quite naturally, the change of effects of public disclosure differ when other alternatives of extended public disclosure would be implemented. This chapter discusses various building blocks for constructing alternative public disclosure regimes and discusses to what extent these building blocks lead towards a change in the private and public effects. Below you will find deviations of the benchmark and their impact on the social costs and benefits.

It is interesting to note beforehand that all alternative building blocks relative to the building blocks in the benchmark mitigate the effects of public disclosure: they mitigate benefits, but also costs, albeit in a slightly different way.

5.1. Which segment? Disclosing versus a segment of data breaches instead of all available data breaches.

Disclosing a segment of data breaches in a public register, for instance solely the data breaches that have been notified according to Article 34 GDPR, and which are thus already communicated to individuals, and consist (in the Netherlands) of around half of the data breaches that have been disclosed. The effects are the following:

- Relatively less private benefits, because less can be learned. However, the most significant data breaches are still in play, hence this effect is likely to be small.
- Relatively less private costs, for instance communication costs are likely to be lower because solely the data breaches which are already notified to consumers are lower.
- Relatively less public benefits, because there is simply less data to harvest effects such as right to know, sunlight as disinfectant etc.
- But also relatively less public costs, especially notification fatigue but also communication costs on the consumer side.
- Less legal issues because the information is already semi-public.

5.2. Which information? Disclosing pseudonymization of data or name the organization that notified.

When data is anonymized, and by this we mean that the name or the organization that notified has been removed (in addition to the contact details that were never part of the benchmark extended disclosure) and not traceable back to a single organization, there are simply no private benefits and costs of extended public disclosure.

One must say that full anonymization for some instances is not likely to be reached because for instance the severity of the breach in combination with the sector and timing could lead to a determination of the organization that has been breached. However, very significant breaches, which are notified according to Article 34 GDPR, are believed to reach the general public anyway. In that sense, it is better to speak of pseudonymization.

Pseudonymization also has a mitigating effect on public benefits and costs, for instance the right to know (because consumer cannot tie data breaches anymore to organizations) and learning about cyber security. Pseudonymization still allows for research on trends and threats, but causal research related to the effectiveness of cyber security measures will be significantly hampered, because one cannot tie investments of a certain data controller to the impact on data breaches anymore.

5.3. When? Disclosing immediately or after one year

Notification after a certain period of time, for instance one year, would likely reduce (the fear for) reputation damage of the data controller. However, it is not very likely that extended disclosure mitigates the impact of the breach because, usually, there is only a small timeframe in doing so, just directly after the breach. As far as immediate action is concerned, delay of disclosing the data breach also affects social benefits. The benefits of the learning effect will also (albeit slightly) diminish, because some learning effects will diminish due to the fast changing nature of cyber security.

5.4. To whom? extended disclosure to selected parties or the general public

Obviously, when extended disclosure solely occurs to selected parties, the social benefits are also limited to the actions of these parties. For instance, if data is shared with the crime department, this could lead to a mitigation of impact, because the crime department can better prioritize the deployment of their resources.[84] When data is shared with academia, this benefits the learning effect. The data controller could incur some communication costs when interacting with these parties. We should however note that disclosing to selected parties is on the edge of the scope of this report, because such an act could hardly be perceived as 'public disclosure'.

5.5. How? Notifying in an oracle or register

The form of information could also determine the private and social effects of extended public disclosure. When information is presented in the form of an oracle, without providing further context, the public could only access this information when providing some of the data it is looking for, for instance the name of the data controller.[85] Obviously, when it is chosen to have an alternative without the name of the data controller, it would be quite hard to construct an oracle in the case of public disclosure, because no 'tag' can be provided to search for.[86] Because an oracle limits the public access of a data breach, for instance, the societal learning effect regarding these data breaches would diminish. However, the mitigation of the positive effects for society is stronger than the mitigation of negative effects for private parties, since consumers or privacy organizations can still 'hack' an oracle by automatically requesting all data.

That being said, we can conclude that the oracle is especially valuable when consumers need to check whether their personal data is being compromised, but since this kind of data is not available at all in the present notification scheme (no personal information is being shared with the DPA), the value of the oracle would, in our opinion, also be limited.

5.6. Summary of effects building blocks

In table 4 below, a summary of the building blocks is given. Note that the effects which are displayed below are merely indicative for the predicted effects of the building blocks. However, in general it can be observed that all deviations from the benchmark mitigate organizational concerns with extended public disclosure at the cost of less social effects.

84. Interview mr Dick Heerschop.
85. There an example of an 'oracles', see for instance the website haveibeenpwned.com.
86. As said, the data subject will not be in the data base as well in this alternative since we limit ourselves to the data breach information that is currently requested by the DPA.

Table 4: summary effects building blocks

Deviation from benchmark	Private effect	Social effect
1. Which segment? Disclosing solely Article 34 data breaches	+ (less private costs)	- (less social benefits)
2. Which information? Pseudonymization	+ + +	- - -
3. When? Disclosing after a year	+ +	-
4. To whom? To science and crime department	+ + +	- -
5. How? Notification in an Oracle.	+	- -

6. Alternatives

This Chapter discusses several alternatives of extended public disclosure. We constructed several alternatives based on the literature and the interviews with experts. Quite naturally, there is a larger number of alternatives for an extended public disclosure regime, because many more alternatives can be constructed from the five building blocks described in the previous Chapter.

6.1. The Benchmark alternative

The benchmark alternative, which is the starting point for our analysis of private and social benefits in Chapter 4, is constructed as follows:

- Which segment? Public disclosure of the data breach data related to both Article 33 and Article 34 GDPR.
- Which information? Data on an individual data breach level, such as the name of the data controller, the amount of records, the type of data breach, the causes of the breach and the measures taken. This is the information provided in Appendix A, with the exception of the contact details of the individual within the organization that provided the notification.
- When? Public disclosure directly after the breach.
- To whom and how? Public disclosure to the general public in a central register.

Main benefits of this alternative:

1. This solution maximizes the social benefits of extended public disclosure as described in Chapter 4.

Main drawback of this alternative:

1. The experts from industry that are interviewed in the context of this research indicate that they would expect relatively limited support for this alternative. This is related to the high perceived reputation damage of full extended public disclosure according to the benchmark alternative.

6.2. Delayed public disclosure

Delayed public disclosure deviates from the benchmark alternative by disclosing data breaches after one year instead of immediately after the breach. Hence the public data breach register will be supplemented with a delay of, for example, one year.

Main benefits of this alternative:

1. This alternative reduces perceived reputation damage, while keeping most social benefits intact. The feared perceived reputation damage by industry is reduced in two ways. First, when time goes by, the newsworthiness of an event will in general be lower. Secondly, when all data breaches of the previous year are made public in one single instance, each individual data breach will gain relatively less attention, especially because there are a high number of data breaches being notified. This effect is also labelled as 'notification fatigue'.[87]

Main drawbacks of this alternative

1. The high perceived reputation damage of full extended public disclosure according to the benchmark alternative could still exist after a year.

6.3. Full delayed disclosure with selected parties (science, crime department)

In this alternative, only selected parties would get the data breach data after a certain period that has to be determined by the DPA. In practice, research institutions, crime departments and CERT communities could apply for the data at the DPA. When one would opt for this alternative, the DPA should constitute a central point of contact for this procedure.

Main benefits of this alternative:

1. Full delayed disclosure would maximize the learning opportunities (see Section 4.5) for a selected group, while mitigating the effects

87. Nieuwesteeg & Faure (2018).

related to perceived reputation damage.[88] For the purposes of scientific research and it is not necessary that data is publicized immediately. However, one should be aware that open data, such as the data breach data in the U.S., is more likely to capitalize on the resources and knowledge of the various research institutions in the world.
2. Full delayed disclosure with the crime department could aid in prioritizing the resources of fighting cybercrime. Arguably, the delay needs to be shorter, because of the versatile nature of cyber risks. The exact period should be determined with the stakeholders.

Main drawbacks of this alternative:

1. Solely disclosing data breach data to selected parties means that there will be barriers of acquiring the data. This would practically mean that the data will be used less, compared to the alternatives that position disclosure as a form of open data (alternatives 6.1, 6.2 and 6.4.). For instance, U.S. research institutes might not know about collaboration possibilities and could not get access to the data.
2. This solution does have other potential social benefits of public disclosure, such as liability, the right to know and sunlight as disinfectant (see Chapter 4).
3. This alternative requires a role for the DPA in selecting the parties with whom it collaborates in sharing the relevant information, which could raise administrative costs.

6.4. Pseudonymized open access extended public disclosure

A fourth alternative for extended public disclosure would be open access of data breaches, but without naming the organization that notified. This data would not be fully anonymous for some organizations, since other aspects could reveal the name of the organization (For instance, everyone knows what is meant by 'a large oil & gas company in the The Hague region').[89] Completely erasing all characteristics that could possibly lead to the disclosure of an organization would effectively mean no further disclosure than the type of disclosure the Dutch DPA currently provides.

Main benefits of this alternative:

1. Pseudonymized open access extended public disclosure has social benefits regarding to improved analysis of trends in cyber security.
2. Everyone can tap in to this kind of a public data base and use it for research, trend reports and other approaches to learn from data breaches.

Main drawbacks of this alternative:

1. This solution does not utilize other social benefits of public disclosure that include the name of the organization that notified, such as liability, the right to know and sunlight as disinfectant.
2. The social benefits related to determining the effectiveness and efficiency of cyber security strategies are strongly reduced, since data breaches cannot be tied to cybersecurity measures within organizations anymore.

6.5. No extended disclosure

One could also opt for no further public disclosure of data breaches, in combination with research that assesses alternative methods that aim to achieve similar goals of stimulating information diffusion in cyber security. In that case, the status quo of the data breach notification regime remains.

88. In order to ensure the advantage of the mitigation of the effect of perceived reputation damage, one could add the condition that anonymity or pseudonymity remains in scientific publications.
89. One could mitigate this risk by applying broader categories of organizations.

7. Conclusion and recommendations

7.1. Conclusion

Cyber security incidents occur on a daily basis and will continue to occur in the future. Government, industry and individuals must keep up. Their cyber security investment strategy regarding these incidents determines the eventual organizational and societal cost of cyber security. But how do we know what are efficient and effective means to invest in cyber security to keep our organizations secure at acceptable social costs?

One of the main issues in cyber security is the lack of information (diffusion) about the nature of cyber risk and the return on investment of strategies to reduce it. This is caused by the fact that information regarding the nature of cyber risks and the return on investment of cyber security investments is distributed asymmetrically among actors. Often, actors solely have access to their own loss data and cyber security investment data, which is insufficient to generate a complete picture of the costs and benefits of cyber security investments. In order to increase social welfare, this data should be diffused and aggregated. This study investigates one possible method to increase cyber security information diffusion: the extended public disclosure of data breaches.

In short, we can conclude that extended public disclosure is good for society but has net costs for the organization that notifies. However, private costs are largely perceived reputation damage. This points out at a crucial role of the positioning of extended public disclosure. In the context of the 'risk free society', data breach disclosure should not be viewed as a bad thing, but as something society can learn from. If not, there is a risk that the perceived reputational damage related to extended disclosure can reduce the willingness to notify and increase a certain compliance culture. In that sense, perceived reputation damage has a real effect.[90]

This report tried to evaluate the option of extended public disclosure of data breaches. We studied the current form of public disclosure of data breaches, the legality of extended public disclosure and the costs and benefits thereof. Next, we drew several building blocks of a public disclosure regime and came up with several alternatives.

7.2. Avenues for future research by the cyber security council

Along the way of performing this scientific research on extended public disclosure of data breach notification obligation, several other relevant instruments to increase cyber security information diffusion have been mentioned. It would be worthwhile to further examine the comparable effectiveness of those other instruments in stimulating cyber security and information diffusion. In that respect the research into the effects of public disclosure of data breach notification stands still in an infant stage. Many more aspects deserve further attention.

First, there needs to be research in the field of liability and data breaches. There is still an open legal question concerning the issue when and to what extent a data breach can be considered as giving raise to liability of the particular organization under tort law. In this respect the question also arises to what extent standardization of cyber security technology could play an important role in relation to liability issues. If it were for example clear that standard protection against cyber security, available on the market, were not used by a particular organization that was victim of a cyberattack, the question could be asked whether that lack of following a particular standard could as such give raise to tort liability. But equally the reverse question could be asked: if an organization would have implemented a state of the art cyber security level and would nonetheless be victim of an attack, could the compliance with the standard then be used by the organization as a defense in tort law? Those are issues that undoubtedly merit further research.

90. One could also argue that the combined effects of the perceived reputation damage (which is estimated as higher than actual reputation damage) and perceived expected value of the sanction (which is higher than the actual sanction of the GDPR) threat cancel each other out in their distorting effects related to incentives of the disclosure of data breaches, but this issue remains subject for future research.

Secondly, it has been mentioned by experts that there are also possible alternatives for or next to extended public disclosure that are capable of also reaching related goals such as information diffusion in cyber security. In this context, it is relevant to study the effectiveness of the current cyber insurance market. In a well-functioning cyber insurance market, there will also be knowledge accumulation by the insurer through collecting claim data that can be used ex ante (before signing the contract) to transfer knowledge related to best practices in cyber security. But that immediately raises the question of how insurers engage in this knowledge accumulation and risk differentiation and whether they are willing (and allowed) to disclose the information they have acquired.

Thirdly, it the context of disclosure, it is worth to investigate voluntary actions to increase information diffusion in cyber security, such as voluntary notifications, transparency. In that respect again the question arises as to the role of standardization: have particular standards been developed concerning the state of the art in cyber security and to what extent are they largely followed?

Fourthly, empirical research regarding the effects of cyber security breaches, but also of public disclosure in the EU is currently largely lacking. Empirical research is of crucial importance for example to substantiate with scientific rigor the precise private and social costs of preventive measures related to cyber security, but also generally the costs of cyber security breaches and for this topic of course most relevant, the precise private and social costs and benefits related to public disclosure.

Fifthly, it could be very valuable to do extended scientific research towards reputation damage related to data breaches in the EU and for SMEs. This is of crucial importance as it was shown that particular organizations have a strong fear of reputation damage. That stands in sharp contrast to the available (US-based) empirical research, indicating that the costs of reputation damage are substantially lower than is often expected by the organizations concerned. It would be of great importance to provide empirical evidence of the extent of the reputation damage, also to obtain broader support from organizations concerned for public disclosure, with all the related societal benefits.

Literature

Christian Biener, Martin Eling and Jan Hendruk Wirfs, 'Insurability of Cyber Risk: An Empirical Analysis' (2015) 40(1) Geneva Papers on Risk and Insurance: Issues and Practice 131, 158.

Fabio Bisogni, 'Data Breaches and the Dilemmas in Notifying Customers' (2015), presented at The fourteenth Annual Workshop on the Economics of Information Security, Delft, 22-23 June 2015.

Fabio Bisogni, 'Proving Limits of State Data Breach Notification Laws: Is a Federal Law the Most Adequate Solution' (2016) 6 Journal of Information Policy 154, 205.

Fabio Bisogni, Hadi Asghari, Michel J.G. Van Eeten, *Estimating the size of the iceberg from its tip - An investigation into unreported data breach notifications* (2017), presented at the sixteenth Annual Workshop on the Economics of Information Security, La Jolla, 26-27 June 2017.

Mark Burdon, Bill Lane and Paul von Nessen, 'Data breach notification law in the EU and Australia – Where to now?' (2012) 28(3) Computer Law & Security Review 296, 307.

Mark Burdon, Bill Lane and Paul von Nessen, 'The mandatory notification of data breaches: Issues arising for Australian and EU legal developments' (2010) 26(2) Computer Law & Security Review 115,129.

Mark Burdon, Jason Reid and Rouhshi Low, 'Encryption safe harbours and data breach notification laws' (2010) 26(5) Computer Law & Security Review 520.

Huseyin Cavusoglu, Birendra Mishra and Srinivasan Raghunathan, 'The Effect of Internet Security Breach Announcement on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' (2004) 9(1) International Journal of Electronic Commerce 69, 71.

CEPS 'Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges' (2018) from <https://www.cl.cam.ac.uk/~rja14/Papers/ceps-rvd2018.pdf> (accessed 13 July 2018).

Sung Choi and M. Eric Johnson, 'Do Hospital Data Breaches Reduce Patient Care Quality?' (2017) WEIS from < http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_2.pdf> (accessed 9 November 2018).

Benjamin Edwards, Steven Hofmeyr and Stephanie Forrest, 'Hype and Heavy Tails: A Closer Look at Data Breaches' (2016) 2(1) Journal of Cybersecurity 3, 14.

Samson Esayes, 'Breach Notification Requirements Under the European Union Legal Framework: Convergence, Conflicts, and Complexity in Compliance' (2014) 31 J. Marshall J. Info. Tech. & Privacy L. 317.

Sanjay Goel and Hany Hawsky, 'Estimating the market impact of security breach announcements on firm values' (2009) 46(7) Information & Management 404, 408.

Paul de Hert and Vagelis Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 Computer Law and Security Review 179, 194.

Myung Ko and Carlos Dorantes, 'The impact of information security breaches on financial performance of the breached firms: an empirical investigation' (2006) 16(2) Journal of Information Technology Management 13, 20.

Juhee Kwon and M. Eric Johnson, 'The Market Effect of Healthcare Security: Do Patients Care About Data Breaches?' (2015) WEIS from https://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_kwon.pdf (accessed 9 November 2018).

Juhee Kwon and M. Eric Johnson, 'Meaningful Healthcare Security: Does "Meaningful-Use" Attestation Improve Information Security Performance?' (2014) 42(4) MIS Quarterly 1043, 1067 from <https://www.econinfosec.org/archive/weis2014/papers/KwonJohnson-WEIS2014.pdf> (accessed 9 November 2018).

Stefan Laube and Rainer Böhme, 'The Economics of Mandatory Security Breach Reporting to Authorities' (2016) 2(1) Journal of Cybersecurity 29, uses a theoretical model and also involves EU law.

Robert Layton and Paul A. Watters, 'A methodology for estimating the tangible cost of data breaches' (2014) 19(6) Journal of Information Security and Applications 321, 330 also indicate that firms can still grow, while writing-off some expenditures related to reputation damage.

Thomas Lenard and Paul Rubin, 'Much Ado About Notification' (2016) 29 Regulation 44.

Ablon, Lillian, Paul Heaton, Diana Lavery, Sasha Romanosky. "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information." Santa Monica, CA: RAND Corporation, 2016.

Amalia R. Miller and Catherine E. Tucker, 'Encryption and the Loss of Patient Data' (2011) 30(3) Journal of Policy Analysis and Management 534,556 from < http://dspace.mit.edu/handle/1721.1/75854> (accessed 9 November 2018).

Tyler Moore, Scott Dynes and Frederick R. Chang, 'Identifying How Firms Manage Cybersecurity Investment' (2015) Working Paper. Southern Methodist University, Dallas, TX, 1-32.

Deirdre Mulligan, *Security Breach Notification Laws: Views from Chief Security Officer* (Study Conducted for the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, 2007) 23, available through <https://www.law.berkeley.edu/files/cso_study.pdf> (accessed 31 October 2018).

Deirdre Mulligan and Fred Schneider, 'Doctrine for Cybersecurity' (2011) 140(4) Daedalus 70.

NCSL 'Security Breach Notification Laws' (29 September 2018) from <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (accessed 8 November 2018)

Bernold Nieuwesteeg, *The Legal Position and Societal Effects of Security Breach Notification Laws* (1st edn, deLex 2014) 80.

Bernold Nieuwesteeg, 'The Law and Economics of Cyber Security' (2018).

Hulisi Ogut, Srinivasan Raghunathan and Nirup M. Menon, 'Information Security Risk Management through Self-Protection and Insurance' (2005) The University of Texas School of Management 1, 31.

Shari L. Pfleeger, 'A Framework for Security Requirements' (1991) 10 Computers & Security 515, 518.

A. Mitchell Polinsky and Steven Shavell, *Handbook of Law and Economics* (vol. 1, 1st edn, Elsevier 2007) chapter 6.

Sasha Romanosky, David Hoffman and Alessandro Acquisti, 'Empirical Analysis of Data Breach Litigation' (2014) 11(1) Journal of Empirical Legal Studies 74.

Sasha Romanosky, Rahul Telang and Alessandro Acquisiti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30(2) Journal of Policy Analysis and Management 256.

Pierangelo Rosati, Mark Cummins, Peter Deeney, Fabian Gogolin, Lisa van der Werff and Theo Lynn, 'The effect of data breach announcements beyond the stock price: Empirical evidence on market activity' (2017) 49 International Review of Financial Analysis 146, 152.

Paul Schwartz and Edward Janger, 'Notification of Data Security Breaches' (2007) 105(5) Michigan Law Review 913, 915.

Bruce Schneier, 'Breach Notification Laws' (Schneier on Security, 21 January 2009) from <https://www.schneier.com/blog/archives/2009/01/state_data_brea.html> (accessed 9 November 2018).

Aleksandra Vold, 'That's All Folks! Alabama Becomes 50th State With Breach Notification Law' (Thompson Coburn LLP, 11 April 2018) from <https://www.thompsoncoburn.com/insights/blogs/cybersecurity-bits-and-bytes/post/2018-04-11/that-s-all-folks!-alabama-becomes-50th-state-with-breach-notification-law> (accessed 9 November 2018).

Jane Winn, 'Are "Better" Security Breach Notification Laws Possible?' (2009) 24(3) Berkeley Technology Law Journal 1133.

Expert interviews

18 July 2018	Interview with mr. Kas Clark (Dutch National Cyber Security Centre)
19 July 2018	Interview with mr. Rejo Zenger (Bits of Freedom)
19 July 2018	Interview with ms. Lokke Moerel (cybersecurity council)
25 July 2018	Interview with mr. Erik de Jong (Fox IT)
26 July 2018	Interview with mr. Eelco Vriezenkolk (Dutch Authority for consumers and markets)
27 July 2018	Interview with ms. Rina Steenkamp (Dutch Data Protection Agency)
3 August 2018	Interview with mr. Gwendal le Grand (chair of the technology subgroup of the European Data Protection Board)
3 August 2018	Interview with mr. Barend Bon (Dutch Data Protection Agency)
8 August 2018	Interview with mr. Tom Kunzler (Open State Foundation)
16 August 2018	Interview with mr. Hans Wienen (PhD Twente University)
30 August 2018	Interview with ms. Nicole Mallens and mr. David de Nood (VNO-NCW)
11 September 2018	Interview with ms. Bibi van den Berg (member Cyber Security Council)
24 September 2018	Interview with mr. Dick Heerschop (Nationale Politie)
26 October 2018	Interview with mr. Hans Huysen (Haaglanden Medisch Centrum)
26 October 2018	Interview with ms. Luisella ten Pierik (Stedin)
31 October 2018	Interview with mr. Martijn Nykerk (Randstad)
2 November 2018	Interview with mr. Cornelis van der Sluis (Ten Holter / Noordam Advocaten)
5 November 2018	Interview with mr. Bas van Gaal (Océ)

Appendix A

Current notification form in the Netherlands

Table with data that needs to be provided when making a for the notification of data breach at the reporting counter of the Dutch DPA (Autoriteit persoonsgegevens)

https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?0

Subject	Question	Answer
0. About this notification		
	Is it about a new or an existing notification? • New notification • Existing notification	*MC*
	On the base of which legislation do you make this notification? • GDPR *(AVG)* • Dutch Telecommunications Act *(TW)* • Dutch Data Protection Act *(Wbp)* • Judicial Information and Criminal Records Act *(Wjsg)* • The Police Data Act *(Wpg)*	*MC*
1. Contact data and other general information		
1.1 Contact details	Which organization or company concerns it? • Registration number of The Netherlands Chamber of Commerce (KvK); • Name company or organization; • Address; • Zip code; • City	*open*
	In which sector is the organization active? *List of all possible to choose sectors,* options between • Financial services • Health and wellbeing • Education • Public administration • Specialist/other business services	*choose*
	Other sector, namely:..	*open*
	Who notifies the data breach? Name; Function; E-mail address; Phone number; Second phone number	*open*
	Whom can the DPA contact for more information of the notification? Name contact person; Function contact person; E-mail address contact person; Phone number contact person; Second phone number contact person	*open*
	Notifier is contact person	Yes/No
1.2 Involvement other company	Was there another company involved in the data breach? • Yes; Name organization; to which extent was the other organization involved? • No	Yes, with *open* OR NO
2. Timeline		
	Exact date of data breach (if known)	*date*
	Start date and end date of the period in which the data breach was	*date*
	Is the breach still continuing?	Yes/No
	When was the data breach discovered?	*date*

Subject	Question	Answer
3. Nature of data breach		
3.1 Nature of breach	Breach of confidentiality of data?	Yes/No
	Breach of integrity of data?	Yes/No
	Breach of availability of data?	Yes/No
3.2 Nature of incident	What is the nature of the incident where there has been a breach of the protection of personal data? • Device, data carrier and/or paper with data lost or stolen • Letter or post package with data lost or returned opened • Hacking, malware and/or phishing • Data placed at old paper • Data shared oral with a unauthorized receiver • Data still on a discarded device or data carrier • Data accidentally published • Data of wrong customer shown in customer portal • Data send or handed in to wrong receiver • Other	*MC*
	Give a summary of the incident where there has been a breach of the protection of personal data?	*open*
4. Categories of personal data that have been breached		
4.1 Personal data in general	Name; Sex, birthdate and/or age; Citizen service number (BSN); Contact details; Access or identification data; Financial data; (Copies of) passports or other proof of identity; Location data; Personal data concerning criminal convictions and offenses or related security measures; Unknown/other, namely:..	Yes/No
4.2 Special categories of personal data	Personal data showing a person's • Race or ethnic origin; • Political opinion; • Religious or philosophical convictions; • Membership of a trade union; • Data concerning somebody's sexual behaviour or sexual orientation; • Data of somebody's health; • Genetical data; • Biometric data	Yes/No
4.3 Quantity of personal data	How many (possibly estimated) data records ("data registers") are affected by the breach	*open*
5. The group of people whose personal data are involved in the data breach		
	Employers; Customers (current and potential); Pupils or Students; Patients; Minors; Persons from vulnerable groups	Yes/No
	Describe the group of people of whom the data is involved in the breach	*open*
	Of how many persons at least is the personal data involved in the breach?	*open*
	Of how many persons maximum is the personal data involved in the breach?	
6. Measures that are taken before the data breach took place		
	Were the personal data encrypted, hashed, or otherwise incomprehensible or inaccessible to unauthorized persons at the time the breach occurred?	Yes/No/Partly, namely:
	If the personal data were partially incomprehensible or inaccessible, which does it part concern?	*open*
7. Consequences of the data breach		
7.1 Consequences of the breach on the confidentiality, integrity and/or availability of the data.	Unauthorized persons have access to the data	Yes/No
	The data may be misused in an improper or unlawful manner	Yes/No
	Within your own organization incorrect, incomplete or outdated personal data may be used	Yes/No

Subject	Question	Answer
	Possibly incorrect, incomplete or outdated personal data may be re-used for other purposes or passed on to other organizations	Yes/No
	An essential service can temporarily not be granted to the involved individuals	Yes/No
	An essential service cannot be granted to the involved individuals permanent	Yes/No
	Other, namely	*open*
7.2 Physical, material or immaterial damage to those involved	Which consequences can the breach have on the private life of the involved individuals: • Discrimination • Identity theft or fraud • Financial losses • Reputation damage • Loss of confidentiality of personal data protected by professional secrecy • Unauthorized undoing of pseudonymization • Those involved cannot exercise their rights and freedoms	Yes/No
	Other consequences, namely...	*open*
	Give an estimation of the of the possible consequences for those involved 1. Negligible 2. Limited 3. Considerably 4. Very big	*choose*
8. Follow-up actions in response to the data breach		
8.1 Inform those involved	Did you informed those involved of the data breach or do you intend to do it	Yes/No/Not yet known
	When did you reported the data breach to those involved	*date*
	When are you going to report the data breach to those involved	*date*
	What is the content of the notification to the involved individuals	*open*
	How many involved individuals did you informed or do you intend to inform	*open*
	Which communication tool(s) do you use or will you use to inform the involved individuals	*open*
	Why do you refrain from reporting the data breach to those involved: • The measures I have taken before the data breach took place offer sufficient protection to be able to omit the report to those involved • It would require a disproportionate effort to inform each individual involved on an individual basis • After the data breach I have taken measures which make it no longer likely that a high risk for the rights and freedoms of those involved will actually arise • Other, namely:...	*MC*
	If informing all those involved would require a disproportionate effort, explain how you will inform the data subjects by means of a public communication or similar measure	*open*
	Which measures have you taken which makes it unnecessary to inform those involved	*open*
	Which other reasons do you have to not inform those involved	*open*
8.2 Measures to deal with the breach	Which technical and organizational measures has your organization taken to deal with the breach and to prevent further breaches	*open*
8.3 International aspects	Has the breach occurred in cross-border data processing, and is the Dutch DPA the leading supervisor for this processing	Yes/No
	If there is a cross-border data processing, which EU countries are involved	*open*
	Has your organization or company reported the data breach to privacy regulators in one or more EU countries, or do you intend to do so	Yes/No
	Yes, namely:	*open*

Subject	Question	Answer
	Has your organization or company reported the data breach to European supervisors on other reporting duties, or do you intend to do so	Yes/No
	Yes, namely:	*open*
9. Additional		
	Is in your opinion the notification complete: • Yes, the required information is provided and no other follow-up notification is needed • No, there will be a follow-up notification with additional information about this breach	*choose*

Colofon

General report: Centre for the Law and Economics of Cyber Security (Erasmus University Rotterdam) and the Economics of Cyber Security Group (TU-Delft)

Design and layout: James Jardine - www.designyourthesis.com

Erasmus University Rotterdam
Centre for the Law and Economics of Cyber Security

Visiting address
Burgemeester Oudlaan 50

Correspondence address
Postbus 1738
3000 DR Rotterdam,
The Netherlands
clecs@eur.nl

www.eur.nl/esl/research/research-areas/institutes/cyber-security