A de minimis rule for personal data breach notifications in the GDPR

Executive Master's Programme Cyber Security
Thesis of Machiel Bolhuis
Studentnr: s9847588
30 November 2016 DEF2

Abstract

The aim of this thesis is to develop a de minimis rule for the notification of personal data breaches that is included in the European General Data Protection Regulation (GDPR), i.e. the formulation of a quantitative or qualitative threshold below which notification of a personal data breach is not mandatory, because the risk to the rights and freedoms (including the respect for private life and family life) of data subjects will be negligible. Such a de minimis rule will be part of a broader privacy risk classification framework. Article 33 of the GDPR states that personal data breaches have to be notified to the supervisory authority, unless it is unlikely to result in a risk to the rights and freedoms of natural persons, while article 34 of the GDPR states that when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, it will have to be communicated to the data subject. The reference to the risk and high-risk notion is a consequence of the risk-based approach that has been incorporated in the GDPR. Although the GDPR includes references to the notion of risk and high-risk (new technologies, large scale processing of sensitive personal data, automated processing (profiling) and systematic monitoring of a publicly accessible area on a large scale), it does not include a proposal for a privacy risk classification framework. Based on a literature review three categories of qualitative criteria can be identified to formulate a privacy risk classification framework for personal data breach notifications: first the nature of the affected data (such as sensitive or no-sensitive personal data), second the nature and extent of the affected processing (such as number of data subjects affected, cybernation, geographical spread, profiling, (non) structural character of breach and duration of breach) and third adequate security measures to protect the personal data (such as encryption or remote wiping). An online questionnaire has been drafted to collect input to formulate a de minimis rule for personal data breach notifications. 55 national and international privacy and security experts responded to this online questionnaire. Based on their responses a de minimis rule for personal data breach notification can be formulated that includes all of the following conditions (i.e. non-exclusive). There is no need to notify personal data breaches to the supervisory authority (and to communicate it to the individual data subject who is affected) if only public personal data is involved (i.e. risk class 0 as defined by Blarkom and Borking, 2001), it only concerns one individual data source and if the financial damage to the individual data subject is limited to € 500. When personal data is stored on individual devices and data carriers such as laptops, mobile phones, USB sticks and CD ROMs that are stolen or compromised, notification to the supervisory authority (and communication to the individual data subject who is affected) is not necessary when the controller has taken adequate security measures to render the relevant personal data incomprehensible or inaccessible and a back up of the affected personal data is available. A de minimis rule for personal data breach notifications therefore does not include a treshold for the number of personal data items or the number of data subjects that are affected, nor does it include a time or geographical treshold for notification. Also the answer to the question whether the personal data breach did have a structural or occasional character is not relevant for the construction of a de minimis rule.

Contents

Figures

Voorwoord

Voor u ligt de scriptie over het onderwerp ‘a de minimis rule for personal data breach notifications in the GDPR’ als afsluiting van de Executive masteropleiding Cyber Security van de Cyber Security Academy. Een aantal redenen gaf de doorslag om te kiezen voor dit onderwerp dat zich richt op privacy risico classificaties voor het melden van datalekken. Ten eerste zijn er privacy experts die - onder verwijzing naar het feit dat privacy als grondrecht moet worden beschouwd - elke verwerking van persoonsgegevens a priori als problematisch en risicovol zien voor de privacy van de eindgebruikers. Een *rule of reason* benadering zoals in andere rechtsgebieden (bijvoorbeeld het Mededingingsrecht) al gemeengoed is, ontbreekt in het Europese privacy recht. Een meer op het principe van proportionaliteit gebaseerd privacy recht heeft altijd tot mijn verbeelding gesproken, zeker in het tijdperk van big data. Recent is deze discussie in Nederland gestart, bijvoorbeeld in de preadviezen van de Nederlandse Juristen-Vereniging (Moerel en Prins, 2016). Al eerder heeft het Centraal Planbureau hier een goede voorzet voor gegeven (Bijlsma, Straathof en Zwart, 2014). Een op risico gebaseerde meldplicht voor datalekken past in een dergelijk betoog. De tweede reden was dat een classificatie voor privacy risico’s (bijvoorbeeld het verschil tussen risico’s en hoge risico’s zoals opgenomen in de Algemene Verordening Gegevensbescherming) bijna altijd is gebaseerd op het antwoord op de vraag welke maatregelen moeten worden getroffen om de geïdentificeerde risico’s voor de gegevensverwerking te beperken. De vraag wordt nooit gesteld of er ook een categorie voor de verwerking van persoonsgegevens kan worden geformuleerd die geen of verwaarloosbare risico’s voor de privacy van eindgebruikers met zich meebrengt. Een soort de minimis rule (‘safe harbour’) voor de verwerking van persoonsgegevens. De risico-gebaseerde benadering voor de meldplicht datalekken die is opgenomen in de Algemene Verordening Gegevensbescherming, biedt mijns inziens een mogelijkheid om een dergelijke de minimis rule voor de meldplicht datalekken te formuleren. De Autoriteit Persoonsgegevens heeft hier met haar beleidsregels inzake de meldplicht datalekken van 8 december 2015 al een voorzet voor gegeven. De derde reden is dat ik geïntrigeerd raakte door het begrip risico. Met name in het eerste jaar van de opleiding kwam dit begrip regelmatig langs (risk assessment, risk mitigation etc), gecombineerd met een overdaad aan standaarden en methodes. De suggestie werd gewekt dat risico’s exact berekend kunnen worden met behulp van bepaalde standaarden en methodes, terwijl andere bronnen juist betoogden dat dit niet mogelijk is (oa Beck, 1986, 1999, 2006). Risico vormt daarmee mijns inziens een weerbarstig begrip, hetgeen natuurlijk een uitdaging vormde voor nader onderzoek.

Speciale dank gaat uit naar Dani Taboada, Raphaël Gellert en Nathalie Laneret die zo aardig waren om eerdere concepten van commentaar te voorzien, evenals mijn begeleiders Simone van der Hof en Bibi van den Berg. Uiteindelijk hebben al mijn inspanningen geleid tot deze scriptie. Ik wens eenieder veel leesplezier toe.

Machiel Bolhuis
30 november 2016

Chapter 1: Introduction

1.1. The risk-based approach and the GDPR

On 4 May 2016 the European General Data Protection Regulation (GDPR) has been published in the Official Journal of the European Union (OJ L 119, 4.5.2016, p. 1–88). The GDPR shall apply from 25 May 2018. The GDPR contains a risk-based approach that is one of its cornerstones (Schwarz, 2016)(Council of the European Union, 2014)(Article 29 WP, 2014a)(Maldoff, 2016). The risk-based approach means that organizations that control the processing of personal data (known as 'controllers') should implement measures to protect the rights and freedoms of data subjects corresponding to the level of risk of these data processing activities (Hunton & Williams, 2014).

Recital 76 of the GDPR states that the (quote): *'likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing'*. The rights and freedoms of data subjects comprise the respect for private and family life and the protection of personal data (EU Charter, 2000) (ECHR, 1953) (TFEU, 2012). Recital 76 also stipulates that the evaluation of risk should be based of an objective assessment, to determine whether data processing operations constitute a risk or a high risk. Some argue that the risk-based approach of the GDPR is based on the technical definition that risk is a threat of a certain probability (Quelle, 2015; 30). This implies that risks to the rights and freedoms of the data subject can be measured, calculated, classified and evaluated.

The risk-based approach has been reflected in various articles of the GDPR, such as the accountability obligation (article 24), the data protection by design principle (article 25), representatives of controllers or processors not established in the Union (article 27), the obligation for documentation (article 30), security of processing (article 32), the personal data breach notification (article 33 and 34), the data protection impact assessment (article 35) and the prior consultation of the supervisory authority (article 36). The thesis will focus on the articles 33 and 34 of GDPR that oblige the controller to notify personal data breaches to the supervisory authority if these breaches result in a risk to the rights and freedoms of natural persons (article 33) and to communicate the personal data breach to the data subject when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (article 34). This means that there will also be personal data breaches that do not cause any or minimal risk to the rights and freedoms of natural persons and therefore do not have to be notified to the supervisory authorities or communicated to the data subjects. Such a category could be defined as a de minimis rule.

1.2. Scope and meaning of ‘de minimis rule’

The phrase ‘de minimis’ is derived from the Latin sentence de minimis non curat lex, which means that the court should not concern itself with trifles (Peterson, 2002). The ‘de minimis’ concept is also applied in European competition law, state aid legislation and in the European Convention on Human Rights (European Commission, 2014a, 2014b)(European Commission, 2001)(Charter of Fundamental Rights of the European Union, 2000). In all these cases, a de minimis concept is applied to distinguish

less or non-important cases from important cases, i.e. in European competition law a de minimis definition is used to quantify, with the help of market share thresholds, agreements that do not present an appreciable restriction of competition under Article 101 of the Treaty on the functioning of the EU (European Commission, 2014a, 2014b). In the de minimis communication of the European Commission regarding the legality of state aid, the Commission indicates, based on market share thresholds, the circumstances in which it considers that agreements - which may have as their effect the prevention, restriction or distortion of competition within the internal market - do not constitute an appreciable restriction of competition (European Commission, 2001). Finally, article 35, paragraph 3 under b) of the European Charter of Human Right (ECHR) states that the Court shall declare inadmissible any individual application submitted under Article 34 ECHR if it considers that the applicant has not suffered a significant disadvantage (ECHR, 2012). The de minimis rule is further relevant in the field of risk regulation where it is assumed that risks that are highly unlikely to be realized (e.g. where the probability is for instance one in a million) do not need to be regulated (Hojnik, 2013; 28)(Adler, 2007). According to Hojnik (2013) a de minimis rule can have two meanings: a procedural and a substantive one. The procedural aspect is derived from the 'de minimis non curat praetor' principle, in accordance with which the praetor (i.e. judge) does not concern himself with trifles (for instance applied to reduce the workload of courts and supervisory authorities), while the substantive meaning of the rule is based on the principle of 'de minimis non curat lex', i.e. the law does not concern itself with trifles. In this thesis a de minimis rule will be applied as meant by the substantive interpretation, ie a de minimis rule for risks to the rights and freedoms of natural persons that are sufficiently small, in terms of probability and impact, that these can be ignored by law.

A de minimis rule for personal data breach notifications therefore requires the formulation of a quantitative or qualitative threshold below which notification of a personal data breach to the supervisory authority and/or communication to the data subject is not needed, because the risk to the rights and freedoms of data subjects will be negligible. With a threshold is meant the formulation of quantitative or qualitative demarcation points related to the nature, scope, context and purposes of the personal data processing, for instance the number of individuals that is affected by processing of personal data or the processing of certain types of personal data, for instance non-sensitive data. The focus of this thesis will be on the construction of a de minimis rule for personal data breach notifications as part of a privacy risk classification framework.

1.3. Relevance of the research

It is not yet clear how risks have to be assessed within the GDPR framework, including the risks relating to personal data breach notifications. Article 70, paragraph 1 under g) of the GDPR states that the European Data Protection Board (i.e. the successor of the Article 29 Data Protection Working Party) can (quote*): '(..) issue guidelines, recommendations and best practices for establishing the personal data breaches and (…) for the particular circumstances in which a controller or a processor is required to notify the personal data breach'*. Article 70, paragraph 1 under h) of the GDPR states that the European Data Protection Board can (quote*): '(...) issue guidelines, recommendations and best*

practices as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons'. The Article 29 Data Protection Working Party will publish an opinion on the notion of high risk and data protection impact assessment later this year (Article 29 Data Protection Working Party, 2016b). This research will deliver building blocks for the construction of such guidelines, recommendations and opinions. The development of a privacy risk classification framework (including a de minimis rule) will increase the efficiency and creditability of the GDPR and the legal oversight of article 33 and 34 of the GDPR by supervisory authorities. The privacy risk classification framework can also be of use for articles 24, 25, 27, 30, 32, 35 and 36 of the GDPR in which reference is made to the notion of risk and high risk to the rights and freedoms of data subjects.

The instrument of personal data breach notifications is also incorporated in other legal frameworks. Article 34a, paragraph 1 of the Dutch Data Protection Act for instance stipulates that personal data breaches only have to be notified to the Dutch Data Protection Authority if the data breach leads to (a considerable likelihood of) serious adverse effects or to serious adverse effects on the protection of personal data (Dutch Data Protection Authority, 2015). The Directive concerning measures to ensure a high common level of network and information security across the Union (NIS-Directive, 2016) contains an obligation for operators of essential services to notify incidents having a significant impact on the continuity of the essential services they provide and for digital service providers to notify incidents having a substantial impact on the provision of online marketplaces, online search engines and cloud computing services (NIS Directive, 2016, article 14 and 16). The Dutch legislative proposal for Data Processing and Cyber Security Breach Notification (Wet gegevensverwerking en meldplicht cybersecurity, 2016) includes a security breach notification for operators of essential (vital) services to notify security and integrity breaches of information systems that result or can result in a significant disruption of the availability and reliability of a product or service. The privacy risk classification framework and a de minimis rule for the notification of personal data breaches in the GDPR can give guidance for the notification obligations that are included in these legal frameworks. The research will also be relevant for the current evaluation of the revised e-Privacy Directive (Directive 2009/136/EC, 2009). Article 4, paragraph 3 of this Directive includes a personal data breach notification obligation for providers of publicly available electronic communication services. This notification obligation and the revised e-Privacy Directive itself are not based on a risk-based approach; insights from this thesis might be relevant for the evaluation of the revised e-Privacy Directive and the personal data breach notification obligation that is included.

The question how a privacy risk classification framework and a de minimis rule for personal data breach notifications should be constructed, has received no attention yet in the academic literature and research. Any steps in this direction can contribute to the academic debate about the development of such a framework and rule.

1.4. Goal of the research and research question

The goal of the research is to develop a de minimis rule for the notification of personal data breaches to the supervisory authorities and the communication of these personal data breaches to the data

subjects as included in the GDPR. Such a de minimis rule will be part of a broader privacy risk classification framework to categorize the risks that personal data breaches impose on the rights and freedoms of data subjects. The rights and freedoms of data subjects comprise the respect for private and family life and the protection of personal data. Definitions of data protection and privacy both will be used in this thesis as similar concepts.

The central research question is:

- How can a de minimis rule be formulated for the notification and communication of personal data breaches in the GDPR as part of a privacy risk classification framework?

This central research question can be divided in several sub questions:

- What is a personal data breach within the meaning of article 33 and 34 of the GDPR?
- What is the aim underlying the personal data breach notification that is included in the GDPR?
- What is the aim underlying the risk-based approach in the GDPR and how is the risk-based approach incorporated in the GDPR?
- What is a definition of a personal data breach, what is the impact of personal data breaches on companies and individuals (e.g. costs, frequency) and what are the main actors causing personal data breaches?
- How can the risk-notion of the GDPR be defined, taking into account the nature, scope, context and purposes of the processing and damages that can be imposed upon data subjects?
- What qualitative and/or quantitative criteria related to the nature, scope, context and purposes of data processing and imposed damages can be formulated to develop a privacy risk classification framework and a de minimis rule for the notification and communication of personal data breaches as incorporated in article 33 and 34 of the GDPR?
- In what way can security measures such as encryption and remote wiping be incorporated in the privacy risk classification framework and the de minimis rule for the notification and communication of personal data breaches as incorporated in article 33 and 34 of the GDPR?
- To what extent are there lessons to be learnt from the cyber security and data protection domain relating to a risk classification framework and the development of a de minimis rule?
- To what extent can the privacy risk classification framework for the notification and communication of personal data breaches be applied to articles 24, 25, 27, 30, 32, 35 and 36 of the GDPR in which also a risk-based approach is incorporated?
- To what extent can the privacy risk classification framework for the notification and communication of personal data breaches be applied to other legal frameworks that include a personal data breach or similar incident notification obligations (such as the NIS Directive and the revised e-Privacy Directive)?

1.5. Research methodology

Desk research (including literature review) and quantitative and comparative research will be applied as research methodologies. First the GDPR will be analyzed to find out what a personal data breach is

within the meaning of article 33 and 34 of the GDPR, what the underlying aim is of the personal data breach notification obligation and how the risk-based approach is incorporated in the GDPR (Council of the European Union, 2014, 2014a). Next the impact on data subjects and the frequency of personal data breaches will be investigated, and the main actors that are responsible for such breaches to stress the importance of personal data breach notifications (Verizon 2015, 2016) (ACM, 2013, 2014, 2015) (Symantec, 2016) (ITRC, 2015, 2016) (Ponemon Institute, 2015, 2016). The personal data breach notification obligation that is included in the GDPR will be compared with a similar notification obligation that is already included in the revised e-Privacy Directive for providers of publicly available electronic communications services (Directive 2009/136/EC, 2009).

Academic publications, laws and guidelines relating to privacy impact assessments, risk assessment, risk classification and risk management in the data protection domain will be analyzed. Guidelines of the Dutch, French and British Data Protection Authorities will be examined (Blarkom and Borking, 2001)(CNIL, 2012)(CNIL, 2015)(ICO, 2014), and publications of the European Union Agency for Network and Information Security (ENISA, 2011, 2012), the National Institute of Standards and Technology (Brooks and Nadeau, 2015), opinions of the Article 29 Data Protection Working Party (2014a, 2014b), recommendation of the European Commission (RFID Recommendation, 2009), reports of the Centre for Information Policy Leadership (CIPL, 2014, 2014a, 2014b, 2014c, 2016a, 2016b) and already existing legal personal data breach notification obligations in the USA (Californian Security Breach Information Act, 2003) and other countries (Nymity Research, 2016, 2016a, 2016b). The Dutch Data Protection Act (Wet bescherming persoonsgegevens, 2015) and its parliamentary history related to the inclusion of a personal data breach notification obligation will be analyzed, and the guideline of the Dutch Data Protection Authority on the personal data breach notification obligation (Dutch Data Protection Authority, 2015) will be examined. The Cyber Age Privacy Doctrine (CAPD) of Amitai Etzioni (1999, 2015b) will be analyzed to investigate whether his privacy doctrine can be used as input for a privacy risk classification framework for personal data breach notifications. The CAPD is based on three criteria (volume of personal data, sensitivity of personal data and combination of personal data sets) to formulate a USA centric privacy risk classification framework. It will be worthwhile to investigate if the CAPD can be applied to risks related to personal data breaches as included in the European GDPR. These sources will be used to develop a privacy risk classification framework and a de minimis rule for personal data breach notifications.

An online questionnaire will be drafted and send to a sample of national and international privacy and security experts, such as members of the Privacy Committee of the Confederation of Netherlands Industry and Employers (known as VNO-NCW), being the largest employers' organization in the Netherlands, the Regulatory Affairs Commission of the Dutch Data Driven Marketing Association (DDMA) and the risk subgroup of the Centre for Information Policy Leadership (CIPL), a London based think tank. Together they represent the views of privacy and security professionals that are employed by private companies in the Netherlands and Europe. Also some other privacy and security experts will be consulted, such as academics and government officials. The findings of the questionnaire and the draft version of the thesis will be discussed at the risk workshop of CIPL that will

be organized on 19th and 20 September 2016 in Paris as part of the GDPR Implementation Workshop of CIPL. The answers to the questionnaire will be used to define criteria to develop a privacy risk classification framework and a de minimis rule for the notification and communication of personal data breaches.

Comparative research will be applied to analyze the use of risk assessment, risk classification and risk management methodologies and standards in the information security domain. Publications and guidelines of the International Standards Organization (ISO, 2005, 2009, 2011), NEN-ISO (2009) and the National Institute of Standards and Technology (NIST, 2011, 2012) will be analyzed. Existing and proposed cyber security data breach notification obligations and their legal frameworks in Europe will be studied, to investigate whether these sources can be used to develop a privacy risk classification framework for the notification and communication of personal data breaches as included in article 33 and 34 of the GDPR. This related for instance to the European Directive concerning measures to ensure a high common level of network and information security that contains incident reporting obligations for operators of essential services and digital service providers (NIS Directive, 2016) and the Dutch legislative proposal for Data Processing and Cyber Security Breach Notification (Wet gegevensverwerking en meldplicht cybersecurity, 2016) that includes an obligation for operators of essential (vital) services to notify security and integrity breaches of information systems that result or can result in a significant disruption of the availability and reliability of a service or product.

Chapter 2: Definition and impact of personal data breaches

2.1. Definition of a personal data breach

The General Data Protection Regulation (GDPR, 2016) contains in article 4, under (12) a definition of a personal data breach as (quote): '*a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'.* The same definition is included in Article 2, (i) of the revised European e-Privacy Directive as (quote): *'a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.'* (Directive 2009/136/EC, 2009).

2.2. Increasing number and impact of personal data breaches

Verizon (2015, 2016), Symantec (2016), the Identity Theft Resource Center (2015, 2016) and Ernst & Young (2015) present global annual overviews of data breaches. Despite the fact that these publications focus on data breaches in general (and not on *personal* data breaches *per se*), the information that is included in these publications offers a good global overview of relevant trends and data breach categories. Moreover, most data breaches that are included in these reports relate to personal data. Symantec for instance states in its report that names of persons are still the most common type of information exposed worldwide, present in over 78% of all data breaches. Home addresses, birth dates, Government IDs, medical records and financial information are present in the 30% to 40% range. Email addresses, phone numbers, insurance information and user names/passwords appear in the 10% to 20% range (Symantec, 2016; 50). All research reports indicate that the number and impact of data breaches – including personal data breaches – have increased over the last years (Symantec, 2016). The most high profile and recent personal data breaches worldwide are nowadays: Yahoo (500 mln breached accounts), Myspace (360 mln breached accounts), Linkedin (167 mln breached accounts), Vk.com (137 mln breached accounts), Badoo (126 mln breached accounts), Dropbox (103 mln breached accounts) and Tumblr (50 mln breached accounts).[1]

The number of USA data breaches in 2015 totalled 781, according to a report released by the Identity Theft Resource Center (ITRC, 2016). This represents the second highest year on record since the ITRC began tracking breaches in 2005 (ITRC Breach Statistics 2005 – 2015). While the most important motive for data breaches remains financial gain, the ITRC noticed a shift in new motives for obtaining sensitive and private personal data (ITRC, 2015). Symantec (2016; 56) states that (quote): *'As data breaches proliferate and people's lives increasingly move online, we expect to see more regulation and more judicial interest in the protection of individual privacy in 2016 and beyond.'*

[1] The Register, "Security analyst says Yahoo!, Dropbox, LinkedIn, Tumblr all popped by same gang", 30 September 2016, http://www.theregister.co.uk/2016/09/30/fiveperson_hacking_gang_claimed_behind_breaches_of_3bn_logins/

Since June 2012 a personal data breach notification obligation has been included in the revised Dutch Telecommunications Act (Wijzigingswet Telecommunicatiewet, 2012) for providers of publicly available electronic communications services. This as consequence of the implementation of the revised European e-Privacy Directive (Directive 2009/136/EC, 2009) in the Netherlands. This has led to 143 personal data breach notifications at the Dutch Independent Post & Telecommunications Authority in 2012 and 211 (2013), 348 (2014) and 411 (2015) personal breach notifications at the Dutch Authority for Consumers & Markets (Onafhankelijke Post & Telecommunicatie Autoriteit, 2012) (Autoriteit Consument & Markt, 2013, 2014 and 2015). The personal data breach notification obligation that is included in the revised Dutch Data Protection Act (Wijziging van de Wet bescherming persoonsgegevens, 2015) since 1 January 2016 has led to approximately 4700 personal data breach notifications at the Dutch Data Protection Authority until 24 November 2016. A lot of notifications are the result of insecure connections and human errors.[2]

2.3. Personal data breaches and relevant actors

Personal data breaches can be caused by various actors. The Netherlands National Cyber Security Centre (NCSC) identifies eight categories of actors who adversely affect the reliability and security of information and information systems (NCSC, 2015; 27-32). These are: professional criminals, state actors, terrorists, cyber vandals and script kiddies, hacktivists, internal actors, cyber researchers and private organizations.

Reports of Verizon and Symantec show that unintentional personal data breaches caused by employees, represent the largest category compared to other internal and external categories of actors. According to Symantec (2016; 51) in the year 2015 22% of all data breach incidents worldwide were accidentally made public and 10% were caused by insider theft. For the Public Administration the category of the data being made public accidentally was even 64,7% of all breach incidents and 78,4% of all identities (Symantec, 2016; 106). Ernst & Young has stated that careless or unaware employees is one of the top two vulnerabilities, the other one being outdated information security controls or architecture (Ernst & Young, 2015; 7).

Verizon (2015; 31) states that 29.4% of all security incidents worldwide were caused by miscellaneous errors (such as errors made by internal staff, especially system administrators) and 20,6% were caused by insider misuse such as privilege abuse. Similar numbers are reported by Verizon for 2016 (Verizon, 2016; 22). Physical theft or loss also represents a significant category, i.e. 15,5% in 2015 (Verizon, 2015; 31). Data breaches caused by external actors represent smaller percentages overall, such as crimeware (25,1%), web app attacks (4,1%), denial of service (3,9%), cyber espionage (0,8%) and payment card skimmers (0,1%)(Verizon, 2015; 31).

[2] http://www.trouw.nl/tr/nl/39683/nbsp/article/detail/4421103/2016/11/24/Ziekenhuizen-melden-elke-dag-datalek.dhtml

2.4. Costs of personal data breaches

Anderson et al. (2012) make a distinction between direct losses, indirect losses and defence costs to measure the costs of cybercrime. Direct loss is (quote): *'the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime'* (Anderson et al, 2012; 5). Indirect loss is (quote): *'the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime'* (Anderson et al, 2012; 5). Defence costs are (quote): *'the monetary equivalent of prevention efforts'* (Anderson et al, 2012; 6). The cost to society is the sum of direct losses, indirect losses and defence costs. The different cost categories are summarized in Figure 1.

Cost to society	Direct losses	- Costs for companies - Costs for customers and end-users - Financial claims of customers and end-users
	Indirect losses	- Opportunity costs for companies - Decline of stock prices
	Defence costs	- Preventative measures - Compliance and notification - Mitigation measures

Figure 1: Framework for analyzing the costs and losses of personal data breaches (Anderson et al, 2012; 5)

2.4.1. Direct losses

Costs for companies

Every year the Ponemon Institute publishes a report, sponsored by IBM, about the cost of (personal) data breaches. The report that has been published in 2015 is based on a survey that covered 350 companies representing 11 countries (Ponemon Institute, 2015) and 383 companies representing 12 countries in 2016 (Ponemon Institute, 2016; 1). The average total cost of a data breach for the companies participating in this research increased from $ 3.52 million to $ 3.79 million (Ponemon Institute, 2015; 1) and to $ 4 millon in 2016 (Ponemon Institute, 2016;1). Findings of the Ponemon Institute indicated an 29% increase in total cost of data breach since 2013 (Ponemon Institute, 2016; 1). The cost of data breaches due to malicious or criminal attacks increased from an average of $ 159 in 2014 to $ 170 per lost or stolen record in 2016. The total average cost of data breaches associated with detection and escalation increased from $ .76 million in 2014 to $ .99 million in 2015. These costs typically include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors.

Companies can also be sued by affected individuals for damages that are caused by personal data breaches (Baas en van Rest, 2012; 265)(Schwartz and Janger, 2007; 969). The California breach disclosure statute (S.B. 1386), which took effect in 2003, includes a statute's private right of action to failure and sets statutory damages of $ 500 for each failure to notify (Cal. Civ. Code, paragraph 1798 84(c) (West. Supp. 2006)). Data about class actions relating to personal data breaches is not available. The threat of class action lawsuits is likely, however, to stimulate companies to admit data

leaks (Schwartz and Janger, 2007; 969). If companies do not notify personal data breaches to the supervisory authorities and data subjects, each affected individual can claim a penalty of $ 500 which can add up to a significant total amount based on a class action lawsuit that includes a large number of participants. These claims can be considered to be direct losses for companies as result of the personal data breaches.

Costs for customers and end-users

The Rand Corporation has published a report about the consumer attitudes toward data breach notifications and loss of personal data, that also includes data about the perceived costs that are related to personal data breaches (Ablon, Heaton, Lavery and Romanosky, 2016). Such costs are for instance nonreimbursed theft of money from checking or savings accounts, time and money spent repairing damaged and compromised credit accounts, lost wages, or the transaction costs incurred from finding a new company with the same services.

The responses to the survey of the Rand Corporation suggest that a substantial number of consumers experience little to no financial loss, while a smaller number of consumers experience large losses; 32% of respondents reported that the breach imposed no dollar loss to them, and, for those who reported a loss, the median was $ 500. Just under 6% of the respondents reported that the inconvenience cost them $10,000 or more. Anderson et al. (2012) have identified significant losses that are related online payment card fraud and online banking fraud (Anderson et al., 2012; 8-9). The direct loss estimations range from annual $ 76 million in the UK to an annual total amount of $ 1,7 billion worldwide (Anderson et al., 2012; 24).

2.4.2. Indirect losses

Opportunity costs for companies

The Ponemon Institute (2015) has defined a separate cost category that relates to the consequences of lost business as result of personal data breaches. Lost business has potentially the most severe financial consequences for an organization. The cost increased from a total average cost of $ 1.33 million in 2014 to $ 1.57 million in 2015. This category can best be placed under the heading of reputational damage that leads to increased customer churn and higher customer acquisition costs. Increasing awareness of identity theft and consumer's concerns about the security of their personal data following a breach also will lead to revenues being lost. These cost categories can be considered as opportunity costs, i.e. costs resulting from lost business opportunities as a consequence of negative reputation effects after the breach has been made public.

Decline of stock prices

Acquisti, Friedman and Telang (2006) have analyzed privacy incidents and information relating to data breaches from different sources for the 1999-2006 (until March) period and investigated the impact of personal data breaches on the market value (i.e. stock market value). The data indicates that there

exists a negative and statistically significant impact of data breaches on a company's market value on the announcement day of the breach. A recent example of the impact of a personal data breach on the shares on the stock market is the hack of TalkTalk in the United Kingdom that took place in the autumn of 2015. Shares of TalkTalk fell almost 5% on 23th October 2015 after the company announced that a significant number of its 4 million customers had been affected by a cyber attack that resulted in data being compromised or stolen. Shares in the company closed down a further 4% caused by statements of executives that it could be a jihadi-inspired attack. On October 26, 2015 the shares of TalkTalk fell a further 12% to hit a two-year low.[3] This sharp decline in the share price was mainly attributed to mismanagement and miscommunication of the hack. According to TalkTalk the cyber-attack could cost it up to £35m in one-off costs.[4] The most recent personal data breach is the Yahoo! hack in which information associated with at least 500 mln user accounts was stolen.[5] This has led to a decline of the Yahoo! shares from $ 44,15 on 22 September 2016 to $ 42,29 on 26 September 2016, a decrease in the share price of 4,2% leading to a reduction of the market capitalization with almost $ 2 bln. Also Verizon apparently requested for a $ 1 billion discount off its pending $ 4.8 billion agreement to buy Yahoo, on top of a $ 1 billion reserve that Verizon may set aside to fund possible liabilities associated with the Yahoo email hack.[6]

2.4.3. Defence costs

Preventative, compliance and mitigation costs for companies should be taken into account, for instance to comply with mandatory personal data breach notifications (European Commission, 2013) (Wijziging Wet bescherming persoonsgegevens en Telecommunicatiewet, 2013). Also additional investments to prevent or mitigate the impact of personal data breaches should be taken into account. The impact assessment that accompanied the NIS Directive stated that the expected costs related to the notification of security breaches to the regulatory authority would be € 125 per individual breach notification, leading to a total cost for notifying breaches on an annual basis of € 212500 at the EU level (NIS Directive, Impact Assessment, 2013; 53). The costs related to cooperating with the regulatory authority in case of specific investigations would in the worst case scenario amount up to a cost for business of maximum € 250000 per investigation, or € 4.25 million to € 8.5 million per year across the EU. The mandatory personal data breach notification that is included in the GDPR is comparable to the breach notification that is included in the NIS Directive, so it is likely that the costs for the personal data breach notification will be similar within the European Union.

2.5. Conclusion

The total number of personal data breaches worldwide has increased over the last years (Symantec,

[3] TalkTalk share price plunges twice as deep as Sony, Carphone Warehouse, Barclays and EBay after cyber attacks, Friday 13th November 2015, http://www.cityam.com/228714/talktalk-share-price-plunges-twice-as-deep-as-sony-carphone-warehouse-barclays-and-ebay-after-cyber-attacks
[4] TalkTalk hack to cost up to £35m, http://www.bbc.com/news/uk-34784980
[5] Press Release of Yahoo! "An Important Message to Yahoo Users on Security" dd. 22 September 2016 https://about.yahoo.com/press-release?key=important-message-yahoo-users-security-182800027&region=US&lang=en-US
[6] Verizon wants $1B discount on Yahoo deal after reports of hacking, spying, October 6, 2016 http://nypost.com/2016/10/06/verizon-wants-1b-discount-on-yahoo-deal-after-hacking-reports/

2016) (Verizon 2015, 2016) (The Identity Theft Center, 2015, 2016). Also the total amount of (financial) costs for companies worldwide related to personal data breaches has significantly increased in the recent past (Ponemon Institute, 2015, 2016). Unintentional personal data breaches caused by employees, represent the largest category compared to other internal and external categories of actors (Symantec, 2016)(Verizon, 2015).

The overview of the costs of personal data breaches present an rude estimate of the losses and costs that are inflicted upon companies, customers, end-users and society. Companies bear the biggest burden of direct, indirect costs and losses and defence costs related to personal data breaches. Indirect costs and losses such as lost business and loss of customer trust and defence costs are very substantial (Anderson et al., 2012). Also end-users can be affected by personal data breaches; results of research by the Rand Corporation indicate that a small number of consumers experience large losses, while a substantial number of consumers experience little to no financial losses (Ablon, Heaton, Lavery and Romanosky, 2016).

Chapter 3: The risk-based approach and the GDPR

Risks in society are everywhere. They come from many sources, including crime, diseases, accidents, terror, climate change and finance and can be caused by various sources such as human actors, system failures and security breaches. Risks can affect individuals (physical harm/ non-physical harm), organizations (such as financial risks) or even affect society (such as loss of trust) (CIPL, 2014b; 14). The focus of this thesis is on the risks that are imposed on the rights and freedoms of data subjects that are related to personal data breaches, in particular the respect for private and family and the protection of personal data. Risks to organizations and society are therefore excluded from the scope of this thesis.

3.1. Probability and harm to the rights and freedoms of data subjects

The general notion of risk is defined as (quote): *'a measure of the uncertainty about the ultimate consequences of a particular activity'* (Chicken and Posner, 1998; 11). The first question is whether, and if so to what extent, risks can be determined, classified and/or calculated. Risk assessment itself can range from the qualitative views of a layman to the views of the expert who is able to give a precise quantitative assessment of the risk (Chicken and Posner, 1998; 1). There is no universally agreed set of rules applicable to evaluation of risk. Most of the time however, risk is defined as set of probabilities and harm that is caused by a threat (NIST, 2012; 6)(Chicken and Posner, 1998; 7)(CNIL, 2012; 8)(CIPL, 2016b; 17)(PRESCIENT, 2012; 68)(Roeser et al, 2013; 35). Such definition has the upside that risks can be measured and evaluated. This approach can be defined as 'technical risk assessment', i.e. a risk is a threat of a certain probability (Quelle, 2015; 30). Related to processing of personal data, this would imply that risk is calculated as the likelihood that the rights and freedoms of data subjects are affected. However neither uncertainty nor severity of outcomes are easily measured or defined (Roeser et al, 2013; 35); the exact calculation of risk is prone to complications.

As all data processing operations can be considered, with some probability, to adversely affect the rights and freedoms of individuals, any processing of personal data would constitute a certain risk to the individual data subject (Quelle, 2015; 26). The specific likelihood and severity of these risks (high risks, low risks etc.) remains to be determined (if possible: calculated) and classified. The goal of this thesis is to investigate if a de minimis rule for personal data breach notification can be defined, as part of a privacy risk classification framework. This necessitates that high-risks related to personal data breaches should be distinguished from risks, low-risks or even (if possible) from negligible or no-risks that are inflicted upon the rights and freedoms of data subjects.

3.2. Technical risk assessment and privacy risk classification framework

In the previous paragraph the use of a ‘technical risk assessment’ that is based on the likelihood and severity of a threat, has been discussed. The next step would be to formulate a privacy risk classification framework, based on which high risks, risks, negligible and even no-risks to the rights and freedoms of data subjects related to personal data breaches can be distinguished. One way to differentiate risks to the rights and freedoms of data subjects related to personal data breaches and to

create a privacy risk classification framework, would be to apply the 'knowledge condition' and 'damage condition' (Quelle, 2015; 27). Both criteria can be applied to differentiate risks, based on the level of knowledge regarding the probability or severity of the threat (knowledge condition) or by requiring the risk to be of greater probability or severity (damage condition). For instance high risks related to processing of personal data should have a high likelihood and high severity, while low- or negligible risks should have a low likelihood and a low severity.

A technical risk assessment that is based on risk being defined (and classified and/or calculated) by the probability and the harm that is caused by a threat, seems to fit the risk-based approach of the GDPR. Recital 76 of the GDPR refers to the likelihood and severity of the risk to the rights and freedoms of the data subject that should be determined by reference to the nature, scope, context and purposes of the processing. Moreover recital 76 states (quote): *'risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.'* Recital 76 therefore implies that a privacy risk assessment should be based upon the notions of likelihood and severity, by the reference to the nature, scope, context and purposes of the processing, and that an objective assessment should be applied to identify the risks. Also article 35, paragraph 4 and 5 of the GDPR that stipulates that supervisory authorities have to publish a list of processing operations for which a Data Protection Impact Assessment (DPIA) is obliged, and may publish a list of processing operations for which no DPIA is necessary, implies that the risk-level of processing operations can be determined, classified and/or calculated. The GDPR however does not give any guidance for the calculation of the risks and only very limited guidance regarding privacy risk classification; it only makes explicit reference to high-risk processing activities.

Three forms of analysis can be applied to identify risks within the framework of a technical risk assessment: qualitative analysis, semi-quantitative analysis and quantitative analysis (Information and Privacy Commissioner, 2010; 12-13). When qualitative analysis is applied, words are used and descriptive scales to assess the relative magnitude of identified risks. It is flexible and used when numerical data is not available or inadequate. Semi-quantitative analysis applies a numeric score (e.g. "1"= Rare, "5"= Almost certain) with a ranking on a descriptive scale and results in a more structured ranking of risks compared to a qualitative analysis. A quantitative ranking applies actual numeric values to express specific consequences and probabilities of outcomes, for instance in monetary terms. A quantitative analysis is generally difficult to apply and requires a lot of research and data collection.

3.3. Non-technical risk assessments out of scope

As described in the previous paragraphs, the privacy risk classification framework and the de minimis rule for personal data breach notifications will be based on a technical risk assessment, i.e. likelihood and severity of threats. This implicates that other alternative risk assessment models such as the concept of world risk society (Beck, 1986, 1999, 2006) and the notion of Black Swans of Taleb (2012)(Taleb, Goldstein and Spitznagel, 2009) will not be applied. Beck stresses the limitations of the technical risk assessment method and focuses on the presumption that risk is a socially constructed

phenomenon. The notion of risk is an inherent feature of modern society, caused by the transformation from an industrial to a modern society (Boutellier, 2005). Risk in modern society is not any more determined by the likelihood and impact, but a social construct created by the inherent dynamics of the modern society (i.e. struggle for power)(Beck, 2006; 334). Modern society generates its own risks ('risks breeds risks')(Van den Berg, 2016). Taleb has introduced the concept of Black Swans: an event that stresses the impact of the highly improbable and cannot be predicted. Such unforeseen events can occasionally happen and reduce the added value of predictions (Roeser et al, 2013; 43). The occurrence of Black Swans limits the value of risk assessments and risk classifications based on a technical risk assessment, because Black Swans cannot be predicted, nor calculated. Taleb states that risk management (quote): *'(....) should be about lessening the impact of what we don't understand - not a futile attempt to develop sophisticated techniques and stories that perpetuate our illusions of being able to understand and predict the social and economic environment.'* (Taleb, Goldstein and Spitznagel, 2009; 1). Also Frick (2012) has raised similar concerns.

The precautionary principle will not be discussed in this thesis. The precautionary principle relates to measures or actions that need to be taken in cases when the risk cannot be quantified because of the lack of scientific data or inadequate scientific data (European Commission, 2002). It applies when scientific uncertainty excludes a full assessment of the risk; the uncertainty both can relate to the likelihood and severity of threats, for instance when cause-effect relationships are likely and suspected, but have not been demonstrated (European Commission, 2010; 14). The precautionary principle originally has been applied to environmental protection and human, animal and plant health, but has also been applied to the privacy and data protection domain (Thierer, 2014). The precautionary principle should be considered as generic safety net, because - although scientific evidence underpinning the risks is not conclusive - it is deemed necessary to take (precautionary) measures. The precautionary principle therefore seems to preempt the formulation of a privacy risk classification framework and a de minimis rule that is based on a technical risk assessment method (i.e. risk-calculation and risk-classification). As stated in the previous paragraphs of this chapter, the risk-based approach of the GDPR however seems to support such a technical risk assessment method, thereby excluding the use of the precautionary principle.

3.4. First proposal of the General Data Protection Regulation (2012)

The first proposal of the GDPR was published on 25th January 2012 (European Commission, 2012). This proposal already included some articles that related to the risks relating to processing of personal data, such as the security of processing in article 30 of the proposal. Furthermore, the proposal promoted the abolishment of the existing obligation to notify *all* personal data processing activities to the supervisory authorities and to replace this general notification obligation by a procedure which focuses on the processing operations which are likely to present *specific risks* to the rights and freedoms of data subjects. In such cases, according to article 33 of the proposal, a data protection impact assessment should be carried out by the controller or processor prior to the processing, which should include security measures to ensure the protection of personal data. According to the second paragraph of article 33, processing operations that present specific risks were (quote):

- *'a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;*
- *information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*
- *monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;*
- *personal data in large scale filing systems on children, genetic data or biometric data;*
- *other processing operations for which the consultation of the supervisory authority is required.'*

The supervisory authority should be consulted prior to the consultation if a data protection impact assessment indicates that processing operations which involve a high degree of specific risks to the rights and freedoms of data subjects, might not be compliant with the Regulation. The prior consultation of the supervisory authority also should include proposals to remedy such situation. If the supervisory authority concludes that the risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy the non-compliance (recital 74, European Commission (2012)).

Articles 31 and 32 of the proposal that dealt with the notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subject did not include any threshold. According to article 31 of the proposal, *all* personal data breaches had to be notified without undue delay and, where feasible, not later than 24 hours after having become aware of it, to the supervisory authority. Article 32 stated that where the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall communicate the personal data breach to the data subject without undue delay. Recital 67 included some examples of the circumstances when a personal data breach should be considered as adversely affecting the personal data or privacy of a data subject such as identity theft or fraud, physical harm, significant humiliation or damage to reputation.

3.5. First reading of European Parliament

In its first reading the European Parliament incorporated a separate article that included an overview of processing operations that were likely to present specific risks (article 32a, respect to risk)(LIBE Committee, 2013). For these processing operations a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects should be carried out. The risk analysis could then trigger a data protection impact assessment as included in article 33. The following processing operations were listed in article 32a as likely to present specific risks (quote):

- *'processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;*
- *processing of special categories of personal data, location data or data on children or employees in large scale filing systems;*
- *profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;*
- *processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*
- *automated monitoring of publicly accessible areas on a large scale;*
- *other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);*
- *where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject; '*

Interesting to note is that the European Parliament added a quantitative threshold regarding processing operations that are likely to present specific risks and for which a data protection impact assessment should be carried out, i.e. processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period. The European Parliament did not propose any changes to the articles that dealt with the personal data breach notifications. Personal data breaches however were listed in article 32a as 'processing operations' that presented specific risks for which a risk analysis and a data protection impact assessment should be carried out.

3.6. Proposal of the European Council

On 3 October 2014 the Italian Presidency sent a proposal to the Council of the European Union to revise Chapter IV of the Regulation that included the articles relating to personal data breach notifications and the data protection impact assessments (European Council, 2014b). This proposal was based on a former proposal that was sent by the General Secretariat of the Council to the Delegations regarding the so-called risk-based approach (European Council, 2014a). The reason for the risk-based approach was the ambition to reduce the administrative burden/compliance costs for companies and to limit the number of notifications of personal data breaches that will be sent to the data protection authorities (Italian Presidency, 2014)(Council of the European Union, 2014a). The underlying notion of the Council's position about risk was that different data processing activities will often have different consequences and deserve a different treatment (Ustaran, 2014).

The proposal of 3 October 2014 included a broad definition of risks to the rights and freedoms of individuals. Recital 60a of the proposal contains an extensive list of risks that may result from processing activities, such as risks that (quote): *'(…) could lead to physical, material or moral damage (…) or any other significant economic or social disadvantage; (…) where data subjects might be deprived from exercising control over their personal data; (…) where personal data are processed*

which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; (…) where personal aspects are evaluated (…) in order to create or use personal profiles; where personal data of vulnerable individuals, in particular children, are processed; where processing involves a large amount of personal data and affects a large number of data subjects.'

The risk-based approach as incorporated in the proposal led to the revision of various articles, such as the incorporation of the risk-based approach in the context of the principle of accountability (article 22), data protection by design and by default (article 23) and article 25 that stipulated that data controllers that are established outside of the European Union do not need to appoint a representative in the European Union for processing activities that are occasional and unlikely to result in a risk to the rights and freedoms of individuals. Article 28 regarding records of personal data processing activities, stated that keeping of such records is not obliged for an enterprise or a body employing fewer than 250 persons, unless the processing is likely to result in a high risk for the rights and freedoms of data subjects.

The concept of high-risks which is referred to in Article 28 and recital 60b) of the proposal, is also introduced for the notification of personal data breaches to the supervisory authority (article 31), the communication of personal data breaches to the data subjects (article 32), data protection impact assessments (article 33) and the requirement to consult with data protection authorities prior to starting processing activities (article 34). High risk for the rights and freedoms of individuals is referred to in articles 28, 31, 32 and 33 as (quote) *'discrimination, identity theft or fraud, financial loss [breach of (…) pseudonymity], damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage'*. Recital 74 of the proposal states that (quote): *'(...) high risks are likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realization of (...) damage or (...) interference with the rights and freedoms of the data subject'*.

Notification of personal data breaches to the supervisory authority should take place not later than 72 hours after having become aware of it; communication to the data subject without undue delay. Notification to the supervisory authority and communication to the data subject is not required when (quote): *'the controller (...) has implemented appropriate technological and organisational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is no authorized to access it, such as encryption; or the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects (...) is no longer likely to materialize.'* (European Council, 2014b, article 32, paragraph 3).

3.7. Statement of Article 29 Data Protection Working Party

In response to the discussions in the European Parliament and the European Council, the Article 29 Data Protection Working Party issued a statement on the role of a risk-based approach in data protection legal frameworks (Article 29 Data Protection Working Party, 2014a). The reason for the statement was that the Working Party was concerned that the risk-based approach was presented as an alternative to traditional data protection rights and principles, and not as a scalable and proportionate approach to compliance. The Article 29 Data Protection Working Party agreed with the principle of the proportionality, i.e. the principle that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk. It also supported the notion that accountability tools and measures (e.g. impact assessment, data protection by design, data breach notification, security measures, certifications) can and should be varied according to the type of processing and the privacy risks for data subjects. According to the Article 29 Data Protection Working Party the nature and scope of data processing has always been an integral part of the application of fundamental principles (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy), so that they are inherently scalable.

However, the Article 29 Data Protection Working Party strongly objected to an interpretation of the risk-based approach that would shift the focus to the use of personal data (and the harm that is caused to data subjects, i.e. the harm-based approach) instead of the collection of personal data itself. According to the Working Party (quote*) 'the risk-based approach goes beyond a narrow "harm-based approach" that concentrates only on damage (…)'* (Article 29 Data Protection Working Party, 2014a; 3). The Article 29 Data Protection Working Party stressed that protection of personal data is a fundamental right according to Article 8 of the Charter of Fundamental Rights and that this right always should be respected by data processors and data controllers. This is the rights-based approach, i.e. data protection is a fundamental right of the EU (Lynskey, 2015; 35). While the Article 29 Data Protection Working Party acknowledged that risk has always been part of the privacy and data protection legislation (i.e. measures should be proportional to the related risks), it also seemed to fear that the risk-based approach as incorporated in the GDPR, might restrict the rights and freedoms of the data subjects compared to the current legislation. Other people argued that the risk-based approach in the data protection domain has been the cornerstone of privacy and data protection legislation since its beginning, so old wine in new bottles and nothing to be afraid of (Gellert, 2015)(Tancock, Pearson, Charlesworth, 2010).

3.8. Publication of the final GDPR

Most risk-based provisions that were included in the proposal of European Council are also included in the final GDPR that was published in the Journal of the European Union on 4 May 2016 (OJ L 119, 4.5.2016, p. 1–88). The concept of the risk-based approach as proposed by the European Council (2014b), has remained more or less the same.

The only significant changes relate to article 33 and 34. In the final GDPR notification of a personal data breach to the supervisory authority is necessary, unless the personal data breach is unlikely to result in a *risk* to the rights and freedoms of natural persons. This means that the threshold of *high risk* for the notification of personal data breach to the supervisory authorities as was included in the proposal of the European Council, has been lowered to *risk*. The threshold of high risk for the rights and freedoms of individuals is still incorporated in the articles that deal with the communication of a personal data breach to the data subject (article 34) and the data protection impact assessment (article 35).

In the final GDPR communication of personal data breaches to the data subject is exempted when the controller has implemented appropriate protection measures. Notification of personal data breaches to the supervisory authorities when appropriate protection measures have been implemented, however is still mandatory and not exempted, as was the case in the previous proposal of the European Council.

The description of high risk that was included in both the two data breach articles (and the data protection impact assessment article) of the proposal of the European Council, ie (quote*): '(…) high risk for the rights and freedoms of individuals, such as discrimination, identity theft and fraud, financial loss, damage to reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage'*, has been eliminated from the final text of the GDPR. This probably has been done to offer the European Data Protection Board (the successor of the Article 29 Data Protection Working Party) more leeway to issue guidelines, recommendations and best practices for establishing personal data breaches, for the circumstances in which a controller or a processor is required to notify the personal data breach and to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in article 34 of the GDPR. The authority for the European Data Protection Board to issue such guidelines, recommendations and best practices is included in article 70, paragraph 1 g) and h) of the GDPR ('Tasks of the Board').

In the final GDPR the notion of high risk for data protection impact assessments is still focused on various and combined criteria such as new technologies that should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level, which could affect a large number of data subjects and are likely to result in a high risk, for example, on account of their sensitivity (GDPR; recital 89 and 91). Article 35 of the GDPR both includes a duty for supervisory authorities to publish a list of processing operations which are subject to a requirement for a data protection impact assessment (article 35, paragraph 4) and the legal power for these authorities to publish a list of processing operations for which no data protection impact assessment is required (article 35, paragraph 5).

3.9. Conclusion

Recital 76 of the GDPR refers to the likelihood and severity of the risk to the rights and freedoms of the data subject that should be determined by reference to the nature, scope, context and purposes of

the processing and that these risks should be evaluated on the basis of an objective assessment. A technical risk assessment that is based on risk being defined (and calculated) by the probability and the harm that is caused by a threat, seems to fit such a risk-based approach.

The GDPR's explanatory memorandum stresses the broad scope of the risk-based approach to the rights and freedoms of natural persons. This should not be a surprise, as almost every data processing operation will, with some likelihood, interfere with a right or freedom (Quelle, 2015; 30). The risk-based approach includes the prevention of social harm to the individual, including physical harm, significant humiliation or damage to reputation when a personal data breach is not addressed in an appropriate way (Tana, 2013). The risk-based approach as defined in the GDPR however does not cover the impact of risks on society or on organizations, but is limited to the risks relating to the rights and freedoms of individuals (including the respect for private and family life and the protection of personal data). The GDPR does not include a proposal for a privacy risk framework. It only mentions the notions of risk and high risk and related data processing activities without any explicit reference to a low or a no-risk category of data processing. The GDPR however seems to suggest that such low or no-risk categories can be identified, because article 30 of the final GDPR lifts an enterprise or organization with fewer than 250 employees from an obligation to maintain records regarding data processing when such activities are not likely to result in a risk for the rights and freedom of the individual, processing is occasional or the processing includes non-sensitive personal data (Schwarz, 2016). Article 35, paragraph 5 of the GDPR states that the supervisory authority may publish a list of processing operations for which no data protection impact assessments is needed. As data protection impact assessments are to be carried out in case of data processing that results in high risks to the rights and freedoms of natural persons, such an article 35, paragraph 5 exemption list would imply that there are data processing activities that only cause risks, low risks or even no risks.

The high-risk category was absent from the Commission's original proposal of January 25, 2012 (Schwartz, 2016). The European Council introduced the high-risk concept as part of the risk-based approach to reduce the administrative burden/ compliance costs for companies and to limit the number of notifications of personal data breaches that will be sent to the data protection authorities (Italian Presidency, 2014)(Council of the European Union, 2014a). As a consequence, the Council can be considered to be responsible for the introduction of the risk-based approach in EU data protection law (Schwarz, 2016). This despite the fact that the European Commission introduced the notion of *specific risk* in its first proposal that was also meant to take a more selective approach to personal data processing. The leading example of obligations that are triggered by high-risk concerns are the communication of personal data breaches to the data subject and especially the obligation to carry out a data protection impact assessment. Most examples of high risk processing activities that are included in the GDPR relate to the conditions under which a data protection impact assessment has to be carried out (article 35).

Some authors such as Gellert (2015) and Tancock, Pearson and Charlesworth (2010) state that the risk-based approach is old wine in new bottles. The Article 29 Data Protection Working Party however

argues that the risk-based approach might open the door to a harm-based approach in which the focus shifts from the collection of personal data to the use of personal data, and that the rights and freedoms of data subject might be restricted (Article 29 Data Protection Working Party, 2014a).

The GDPR does not include any specific guidelines to measure, classify and/or calculate the risks and high risks to the rights and freedoms of individuals. The only quantitative reference has been made during the first reading of the European Parliament in which an example of a *specific* risk is defined as processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period (LIBE Committee, 2013). Most (qualitative) guidance in the final GDPR is given for high risk data processing activities for which a data protection impact assessment is necessary (article 35). High risk data processing activities relate to new technologies, large scale processing of sensitive personal data, automated processing (profiling) and systematic monitoring of a publicly accessible area on a large scale. High risk data processing as included in the GDPR, is built upon the point of view that the *combination* of various individual criteria define high risks (e.g. new technology combined with large scale processing of personal data).

How these concepts and notions have to be applied probably will be determined by the European Data Protection Board (the successor of the Article 29 Data Protection Working Party) that has the authority to issue guidelines, recommendations and best practices relating to personal data breaches and the notion of (high) risks (article 70, paragraph (g) and (h) GDPR). The Article 29 Data Protection Working Party also has stated that it will issue guidance for controllers and processors on the notion of high risk, and data protection impact assessments (Article 29 Data Protection Working Party, 2016b). Finally, article 35, paragraph 4 stipulates that the supervisory authorities (i.e. national data protection authorities) shall establish and make public a list of kind of processing operations which are subject to the requirement for a data protection impact assessment. It is therefore likely that before the GDPR has entered into force on the 25th May 2018, there will be more clarity regarding the way the risk-based approach has to be applied in practice.

Chapter 4: Privacy risk classification framework for personal data breach notifications

4.1. What constitutes a risk-based approach in the data protection domain?

As stated in the previous chapters, the risk-based approach of the GDPR means that data controllers should implement measures to protect the rights and freedoms of the data subjects, corresponding to the level of risk of these processing activities (Hunton & Williams, 2014). Relevant instruments that are often applied to assess the risk related to personal data processing, are privacy risk management frameworks and privacy risk assessments (also referred to as privacy impact assessments). Privacy risk management can be defined as (quote*): 'the process of systematically identifying, managing and mitigating the impact of a personal data operating on the organization and increasingly on individuals'* (CIPL, 2016b; 6) and includes (privacy) risk assessment as one the necessary steps that should be taken. Risk assessment can be defined as (quote*): 'a scientific and technologically based process consisting of three steps: risk identification, risk analysis and risk evaluation'* (ENISA, 2016, website)(ISO 31000, 2009: 14)(New Zealand Government, 2014; 5). The final step of a risk management framework contains risk treatment that contains risk reduction, risk transfer and risk acceptance (ENISA, 2012; 15)(ISO/IEC 27005:2011; 20-23). The risks that are remaining after the risk treatment has been carried out, are defined as residual risks (ENISA, 2012; 15-16).

The risk management and risk assessment methodologies which are applied in the privacy and data protection domain such as for instance the methodology to carry out a privacy impact assessment (CNIL, 2015)(ICO, 2009)(Information and Privacy Commissioner Ontario, 2010) and the use of a privacy risk management framework (CNIL, 2012) in most cases are inspired by the risk models that are developed and constructed in the risk management and information security domain such as the ISO 31000 standards, ISO/IEC 27000 standards and NIST guidelines for conducting risk assessments (NIST, 2012) and managing information security risks (NIST, 2011).

The assessment of privacy risks is not a stand-alone activity but should be part of generic risk assessment frameworks. The Office of the Australian Privacy Officer for instance has stated that information derived from privacy impact assessments (PIAs) should be applied in the broader context of project risk management processes (OPC, 2006; VII). Also the Information Commissioner's Office (ICO) in the UK has stated that companies should plan PIAs in the context of risk management (ICO, 2009; 5)(Wright and De Hert, 2012; 10). Trilateral Research Consulting considers the integration of privacy risk and PIA into the risk management processes as a necessary pre-condition (Trilateral Research Consulting, 2013; 13). Data protection impact assessments will be (quote*): 'more effective if it is embedded in the general risk management processes.'* (Quelle, 2015; 141).

4.2. Foundation of a risk-based approach in the data protection domain

As referred to in the previous chapter, some people argue that the risk-based approach in the data protection domain is not a new concept (Gellert, 2015)(Tancock, Pearson, Charlesworth, 2010). Reference can be made to the European Data Protection Directive 96/46/EC, for instance to the articles regarding the security of processing (article 17) and the prior checking obligation (article 20). Article 20 of the Data Protection Directive 95/46/EC states that Member States (quote): *'shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof'.*

The legal regime applicable to the processing of special categories of data (e.g. sensitive personal data, article 8) in the Data Protection Directive 95/46 can also be considered as the application of a risk-based approach; strengthened obligations for processing which is considered risky for the affected persons (Article 29 Data Protection Working Party, 2014a). The lawful processing on the ground of legitimate interest of the controller, as included in article 7f) of Data Protection Directive 95/46, also can be considered as risk assessment, because it includes a balancing test to assess whether the legitimate interests of the controllers are overturned by the interests of the data subjects. Privacy principles such as legitimacy, data minimization, purpose limitation, transparency, data integrity and data accuracy already include a proportionality test which lead to risk-based and scalable obligations (CIPL, 2016b; 3)(Article 29 Working Party, 2014a). The principle of proportionality is also included in the GDPR as it states that (quote): *'the right to the protection of personal data is not an absolute right, but must be balanced against other fundamental rights, in accordance with the principle of proportionality'* (GDPR, recital 4).

The assessment of risks relating to processing of personal data has led to the introduction of various instruments and concepts such as privacy risk management frameworks, privacy impact assessments, data protection impact assessment, privacy by design and privacy by default. All these instruments and concepts are applied to determine, classify and/or calculate the privacy risks that are related to the processing of personal data. As first step to discuss the application of a risk-based approach in the data protection domain, it is necessary to shed some light on the differences and similarities between these various instruments and concepts.

A privacy impact assessment, also referred to as PIA, is an instrument to identify and reduce the privacy risks of projects. According to Wright & de Hert (quote): *'a privacy impact assessment can be applied as methodology for assessing the impacts on privacy of a project, policy, program, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders for taking remedial actions as necessary in order to avoid or minimize negative impacts'* (Wright & De Hert, 2012; 5). The foundation of privacy impact assessments has been laid in Canada, Australia, the United States of America and New Zealand. In these countries the instrument of privacy impact assessment was introduced at the end of the last century (Tancock, Pearson and Charlesworth, 2010; 118, 120). The use of privacy impact assessments was also supported by the introduction of Technology Assessments, Impact Statement and Impact Assessments (such as

Environmental Impact Assessments) in the last decades of the previous century (Tancock, Pearson and Charlesworth, 2010; 119)(Holvast, 1986; 196). The UK Information Commissioner's Office (ICO) published the first European Privacy Impact Assessment Handbook in 2007 (ICO, 2009), and the UK Cabinet Office adopted privacy impact assessments as a mandatory measure for all UK government agencies in 2008. Also the publication of the European Commission's Recommendation on Radio Frequency Identification (RFID) in 2009 raised the popularity of a privacy impact assessment (Wright & De Hert, 2012; 4).

Interest for the instrument of privacy impact assessment has increased over the last years (Wright and De Hert, 2012; 3-4), and has become more relevant in the data protection domain as information technology has further developed, and regulators and organizations have focused more attention on accountability for data processing (CIPL, 2014c). According to Tancock, Pearson and Charlesworth (2010, 124) the privacy impact assessment will be applied more often in the future as consequences of new and emerging technologies (such as cloud computing services and social networking technologies). At the same time as the instrument of privacy impact assessment was introduced, other national and international initiatives were taken to create a framework for risk assessment related to the privacy and data protection domain. These initiatives were partly driven by security breach notification laws in Europe, Australia, Canada, New Zealand, the United States (CIPL, 2014c; 6)(ENISA, 2012)(CNIL, 2012) (CIPL, 2014a, 2014b, 2014c, 2016a, 2016b).

In addition to the data protection impact assessment in article 35, the final GDPR also includes a separate article about data protection by design and by default (article 25). With privacy by design is meant the implementation of (quote): *'appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing'* (GDPR, article 25, paragraph 1). With privacy by default is meant that (quote*): 'the controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of personal persons.'* (GDPR, article 25, paragraph 2). By applying a privacy by design approach, organizations can achieve a 'default' modus operandi for privacy protection (Information and Privacy Commissioner Ontario, 2010; 1). Privacy impact assessments are an integral part of a privacy by design approach (Information Commissioner's Office, 2014; 4).

4.3. Building blocks for a privacy risk classification framework

In this paragraph an overview will be given of the most relevant privacy and data protection literature which has touched upon the notion of privacy risk classification. These sources include academic publications, data protection and cyber security legislation, guidelines of national data protection

authorities, other supervisory authorities and think tanks. The overview has not the intention to be all inclusive, but will be limited to the most relevant publications.

4.3.1. Personal data breach notification obligation in revised e-Privacy Directive

The revised European e-Privacy Directive (Directive 2009/136/EC, 2009) was the first European Directive to include a personal data breach notification; it applies to providers of publicly available electronic communications services (ENISA, 2011). According to the revised e-Privacy Directive the notification of personal data breaches (quote): *'reflects the general interest of citizens in being informed of security failures which could result in their personal data being lost or otherwise compromised, as well as of available or advisable precautions that they could take in order to minimise the possible economic loss or social harm that could result from such failures'* (Directive 2009/136/EC, 2009; recital 39). According to article 4, paragraph 3 of the revised e-Privacy Directive the provider of publicly available electronic communications services shall (quote): *'without undue delay, (..) notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the individual of the breach without undue delay'* (Directive 2009/136/EC, 2009; article 4(3)). *'A breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community'* (Directive 2009/136/EC, 2009; recital 61).

The revised e-Privacy Directive does not include a (risk) threshold for the notification of personal data breach notifications to the competent national authorities. This conclusion is confirmed by the Commission Regulation No 611/2013 on the measures applicable to the notification of personal data breaches that stipulates that providers should notify *all* personal data breaches to the competent national authorities. Therefore, no discretion should be left to the provider whether or not to notify personal data breaches to the competent national authority (European Commission, 2013). The Dutch Minister for Security and Justice has stated that the justification of such a general and all inclusive personal data breach obligation can be found in the acceptance that each processing of publicly available electronic communications services involves a substantial risk. Similar risks do not exist for other forms of data processing that are not covered by the revised e-Privacy Directive (Staatssecretaris van Veiligheid en Justitie, 2012; 10).

4.3.2. ENISA and privacy risk classification

In 2011 the European Network and Information Security Agency (ENISA) published its report on data breach notifications in the EU. The purpose of the report was to gather the experiences of various stakeholders (such as regulators and companies) with the data breach notification obligation for the electronic communication sector that was included in the revised European e-Privacy Directive (Directive 2009/136/EC, 2009). ENISA interviewed 15 telecommunications service providers in 12 countries, 18 regulatory authorities in 17 countries and 13 other private organizations and experts in 10 countries. Although the personal data breach notification that is included in the revised e-Privacy

Directive does not include a risk-threshold, the data protection authorities that were interviewed by ENISA, stressed the need for risk-based decisions and prioritization of notifications (ENISA, 2011; 17). According to ENISA, most regulatory authorities did not have any formal criteria for measuring risk; risk assessment was done mostly on an ad hoc basis. Several regulators however did apply quantitative criteria to determine risk, such as the number of people that are affected by the breach and the amount of personal data that was breached. Also qualitative indicators were taken into consideration, such as the type of personal data, e.g. health data, data related to sexual orientation, age (children), criminal offences, political, philosophical or religious beliefs and financial data. Telecom operators that were consulted by ENISA also referred to the need for risk prioritization. Most telecom operators indicated that it was difficult to measure risk, particularly in advance, as many incidents are unique and unpredictable, but stressed the importance to rate incidents based on specific threat levels. In order to prevent 'notification fatigue' for both the operator and the data subjects, telecom operators stated that breaches should be classified according to specific risk levels (ENISA, 2011; 4). Similar to the regulatory authorities, most telecom operators did not use specific methodologies or procedures for determining risk levels, but was done on an ad hoc basis. In some cases, the risk level was based on the type of personal data, the number of data subjects, the quantity of data, age of data and the nature of the breach, i.e. technical, human error, or theft.

Based on the interviews, ENISA recommended that notifications should only be necessary if personal data breaches were likely to cause harm to data subjects or violate their rights. Notification should not be necessary in cases of encrypted data. Furthermore ENISA suggested specific criteria that can be used to prioritize breaches such as the number of people affected, the nature of the personal data that has been breached (financial, health, etc.), the nature of the breach (widespread, or an isolated incident) and the security level (has the data been encrypted). So although the personal data breach notification obligation that is included in the revised e-Privacy Directive does not include a risk threshold, both regulators and telecom operators have tried to define such thresholds to make the notification obligation more efficient and meaningful. The fact that both regulators and telecom operators apparently have tried to work around the strict notification conditions for personal data breaches that are included in the revised e-Privacy Directive, supports the reasonability to include an explicit risk-based approach (and a related risk-threshold) in the GDPR.

As follow-up of its report on data breach notifications, ENISA has published recommendations on technical implementation guidelines of Article 4 of the revised e-Privacy Directive, i.e. the article that includes the personal data notification obligation for providers of publicly available electronic communications services (ENISA, 2012). According to ENISA an organization needs to have a risk management framework in place to be better prepared to prevent, detect and respond to personal data breaches (ENISA, 2012; 14). The method proposed by ENISA in particular focuses on the impact or the 'adverse effect' on the individuals whose personal data have been breached (as specified in the revised e-Privacy Directive) and not on the likelihood of personal data breaches that will take place. ENISA recommends that the following two categories should be considered when assessing the impact / severity of a personal data breach (quote, ENISA, 2012; 24-25):

1. *'Identifiability of data: the ability to identify an individual based on the personal data breached. The easier the identifiability, the higher the impact. In order to determine this, the type of personal data breached has to be identified, e.g. ID data (name, address, data of birth, gender etc) and sensitive data in the sense of article 8 of the Data Protection Directive 95/46/EC.(...)*

2. *Level of exposure accomplished: this will be based on the following:*
    a. *Nature of the data breach, type of exposure: the type of breach that took place, e.g. unauthorised or unlawful access, destruction, alteration / modification, disclosure, transmission, processing, storing, accidental or unlawful loss of personal data.*
    b. *Preventive controls in place: e.g. proper access control, encryption, backups and unintelligible data: the less the effort needed to use the data, the higher the exposure, and the severity of the personal data breach. (...)*
    c. *Delay to identify the breach: The delay in identifying the breach is a parameter worthwhile considering, since the longer the delay the greater the possibility that the exposure levels have increased.'*

ENISA states that the number of people by the personal data breach should not be used as a criterion for assessing the impact of the personal data breach, without given any reason for this point of view. Nonetheless the number of people that are affected by the personal data breach should be determined, because it has to be notified to the competent authority (ENISA, 2012; 25).

Each of the parameters (such as sensitive personal data, nature of the data breach, delay to identify the breach etc.) within the two categories referred to above, is rated based on the severity of its impact. Different scenarios are then constructed by ENISA for different kind of personal data breaches; for instance personal data breaches that include unauthorised or unlawful access to national identifiers that were not encrypted for which the notification has been delayed for 5 days, would get a total score of 7. This approach of ENISA can be considered as *semi-quantitative analysis*, because it associates a numeric score with points on an descriptive scale (e.g. '1' = low/negligible; '6-7' = very high). This contrary to a quantitative analysis that depends upon actual numeric values to communicate specific consequences, for instance expressed in monetary, technical or human terms (Information and Privacy Commissioner, 2010; 13).

A similar approach has been taken by the French Data Protection Authority (CNIL) as part of the implementation of the mandatory personal data breach notification of the revised e-Privacy Directive in France (article 34 bis of the modified Law 78-17 of 6 January 1978). CNIL has published an analysis tool for the assessment of breaches to assist providers of publicly available electronic communications services.[7] This analysis tool is similar to the tool that is proposed by ENISA. To measure the magnitude of the data breach, providers should fill in a matrix that includes the identifiability of the data that has been breached (‘caractère identifiant des données ayant fait l’objet de la violation’) and the harmful nature of the breach on the persons concerned (‘caratère préjudiciable de la violation sur les

[7] https://www.cnil.fr/fr/fileadmin/f_dynamiques/scripts_php/telecharger/Notifications-AutoEvaluation.xls

personnes concernées'). Each of the two criteria can be scored on a scale from 1 (neglectable) to 4 (maximum) and the final score can be calculated for each breach (< 4 is neglectable, =5 is limited, =6 is important and > 6 is maximum).

4.3.3. Cyber Age Privacy Doctrine (Amitai Etzioni)

Professor Amitai Etzioni has introduced the concept of a Cyber Age Privacy Doctrine (CAPD) that can be used by the government to justify collection of personal data, for instance through the use of surveillance cameras. The CAPD is embedded in the American legal framework in which the Fourth Amendment protects its citizens against unreasonable searches by government agencies.[8] In the United States, a person that transfers personal data to a third party, sharing this information with law enforcement officials by this third party does not constitute a Fourth Amendment search. In such cases, the person who transfers information to a third party, is not protected by the Fourth Amendment (Etzioni, 2015b; 21). This contrary to the European data protection legislation that is based upon the notion that any secondary use of personal information released by a person or collected about him requires the a priori consent of the original individual 'owner' of the information. According to Etzioni, courts in the United States therefore solely focus on the question whether the *initial* collection of information was legal. They do not address the fact that legally obtained personal information may be used in a later stage to violate privacy; a practice that is rather common in the current digital world. For these reasons Etzioni has constructed the Cyber Age Privacy Doctrine (CAPD) that is based on a liberal communitarian philosophy that assumes that individual rights, such as the right to privacy, must be balanced against the common good (i.e. public interest), such as health and national security (Etzioni, 2015b; 5)(Etzioni, 1998).

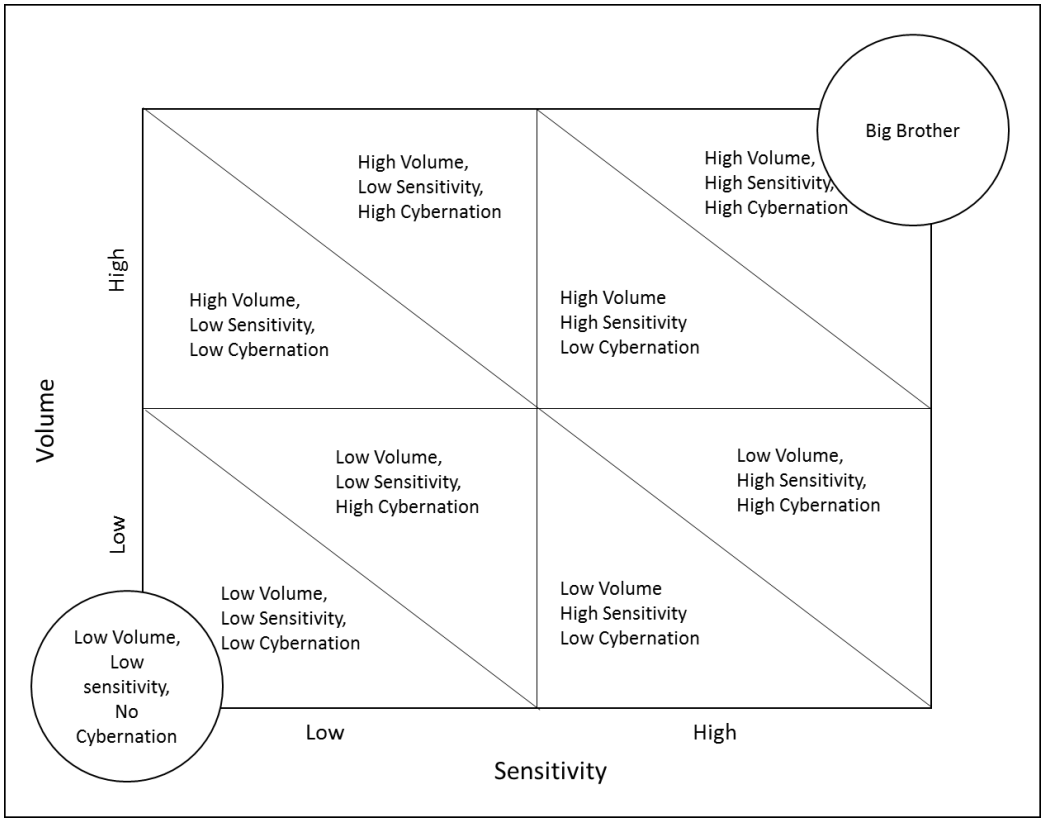
Although the American legal framework regarding data protection and privacy is different from the European framework and the balancing of individual rights and freedoms against the public interest is more difficult to align with the rights-based approach of the European Data Protection Directive 95/46/EC and the GDPR, it nonetheless is worthwhile to investigate the added value of the CAPD for the formulation of a privacy risk classification framework and a de minimis rule for personal data breach notifications. This mainly because the criteria that are applied by Etzioni to formulate his CAPD, are also relevant for other jurisdictions.

The CAPD presents a privacy classification framework along three dimensions: volume, sensitivity and cybernation of personal data. The first dimension (volume) constitutes of two components, namely quantity (quote: *'the amount of information collected, whether this is measured in terms of e-mails, phone records, text messages, or in terms of megabytes of information'*) (Etzioni, 2015b; 27) and bandwidth (quote: *'Collection of only one type of information, such as the metadata associated with an individual's phone calls, emails, or locations, constitutes narrow bandwidth collection. By contrast, the collection of several kinds of information—say, phone call content and voice data and text message content and email content— constitutes broad bandwidth collection'* (Etzioni, 2015a; 1276). Least

[8] The Fourth Amendment is defined as (quote): *'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be limited'* (USA Constitution, Bill of Rights).

intrusive are those personal data collection methodologies or instruments which collect only single pieces of information. The second dimension of the Cyber Age Privacy Doctrine is sensitivity, the level of sensitivity of personal information. For instance, health data is considered highly sensitive, just as political beliefs. The third dimension of the Cyber Age Privacy Doctrine is cybernation, i.e. the process of storing personal information, combining it with other pieces of information ('collating'), analyzing it and distributing it. Combined, analyzed and distributed personal information provides a very intrusive profile of the data subject and causes the most serious violations of privacy. The more information is cybernated, the more intrusive it becomes (Etzioni, 2015b; 12). The Cyber Age Privacy Doctrine "Cube" of Etzioni can be designed based on these three dimensions, as shown in Figure 2. As each of the three dimensions can be rated as high or low, the cube also presents a privacy risk classification framework along three dimensions.

The Cyber Age Privacy Doctrine "Cube"



1. Low Volume, Low Sensitivity, No Cybernation: Tollbooths
2. High Volume, Low Sensitivity, Low Cybernation: Collection of phone records
3. Low Volume, Low Sensitivity, High Cybernation: Household purchases of specific, routine consumer goods
4. Low Volume, High Sensitivity, Low Cybernation: Airport screening devices that reveal the body
5. High Volume, Low Sensitivity, High Cybernation: Select cloud storage
6. High Volume, High Sensitivity, Low Cybernation: Health records
7. Low Volume, High Sensitivity, High Cybernation: Leaks of names of CIA agents
8. High Volume, High Sensitivity, High Cybernation: The sale of data brokers "dossiers" to the government

Figure 2: The Cyber Age Privacy Doctrine "Cube" (Etzioni, 2015b; 37)

4.3.4. Personal data breach notification laws

Laws that include personal data breach notifications have become very popular over the last years. According to Nymity Research (2016a) most European countries have a personal data breach notification obligation incorporated in their laws. More than 30 countries outside the United States require or strongly recommend notification (Hunton & Williams, Cognicion, FireEye, 2016; 15). Also most individual states of the United States of America have implemented a personal data breach notification obligation (Nymity Research, 2016a, 2016b); currently there are 47 personal data breach notifications state laws in place in the United States (Hunton & Williams, Cognicion, FireEye, 2016; recording). The reasons for the increasing popularity for the personal data breach notifications can be summarized as 'Sunlight as disinfectant' and the 'Right to Know' (Maurushat, 2009). This means that the instrument of personal data breaches is used to increase transparency. The benefits of transparency include mitigation of loss and damage in the sense that people who have become a victim of personal data breaches can take remedial actions. Personal data breach notifications also assist controllers, regulators and society to understand the causes of failure, to enable the development of appropriate responses to minimize the risk of future events and their impact. Additionally, personal data breach notifications generate the necessary information that regulators need to perform their supervisory functions (Ustaran, 2012; 159). Some of these laws include specific thresholds that are relevant for the formulation of a privacy risk classification framework. An overview of these laws is presented in this paragraph.

The first law for personal data breach notifications was the California Security Breach Information Act that was enacted in 2003 (Zuiderveen Borgesius, 2011; 210). In some states of the United States disclosure to the authorities only applies when the breach affects more than a certain number of individuals, e.g., 500 in California, or 1,000 in Alaska and Hawaii (Tana, 2013).

In 2014 the Personal Information Protection and Electronic Documents Act in Canada was amended to include provisions that require mandatory reporting of security breaches to both the Privacy Commissioner and the affected individuals (Barabas, 2015; 28). These breaches only have to be reported by the organization to the Privacy Commissioner and the affected individual (quote*): 'if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.' (*Bill S-4, Act to amend the Personal Information Protection and Electronic Documents Act, Division 1.1, Breaches of Security safeguards, Article 10.1). To determine whether the risk threshold is met, the organisation must consider the sensitivity of the personal data and the probability of misuse of the personal data. Harm is defined widely and includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on credit records and damage or loss.

Ireland introduced a Personal Data Security Breach Code of Practice in 2011.[9] Personal data breaches in Ireland do not have to be notified to the Data Protection Commissioner if the breach is notified fully and promptly to data subjects, the breach does not affect more than 100 data subjects and it does not include sensitive or financial data (Hallinan, 2011). Since 2009 article 42a of German Data Protection Act ('Bundesdatenschutzgesetz') limits the personal data breach notification obligation to sensitive personal data, personal data that is protected by professional secrecy such as medical or notarial professional secrecy, personal data related to criminal convictions and personal data related to bank accounts and credit cards. Since 2010 article 24, article 2a) of the Austrian Data Protection Act ("Datenschutzgesetz 2000") limits the personal data breach notification obligation to a category of relative serious cases (quote (translated): *'Such obligation does not exist if the information – taking into consideration that only minor damage to the data subject is likely and the cost of the information to all persons concerned - would require an inappropriate effort'*).

In the Netherlands, on 1 January 2016 the revised Data Protection Act entered into force that includes the obligation to notify personal data breaches to the Dutch Data Protection Authority and affected individuals. A personal data breach must be reported to the Dutch Data Protection Authority if it leads to (a considerable likelihood of) serious adverse effects on the protection of personal data, or if it has serious adverse effects on the protection of personal data (article 34a, paragraph 1, Dutch Data Protection Act). The data breach must also be reported to the data subjects if it is likely to adversely affect their privacy (article 34a, paragraph 2, Dutch Data Protection Act). The reasons to include the threshold for the personal data breach obligation notification are to avoid an unnecessary administrative burden for government and private companies and the presumption that a notification obligation without any threshold would become useless because it would contain meaningless breaches (Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet, 2013; 6). To determine whether a personal data breach would have a considerable likelihood of serious adverse effects on the protection of personal data, in particular the nature and scale of the breach, the nature of the affected personal data and the extent to which technical protection measures have been taken regarding the affected personal data, are deemed to be relevant (Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet, 2014b; 6). In the explanatory memorandum to the revised Dutch Data Protection Act the Dutch Minister for Security and Justice defended the general threshold ("likely to adversely affect") by dismissing the approaches that Germany and Austria have taken. According to the Minister, a limitation to certain categories of personal data, thereby excluding other categories, would create the risk that some processing of personal data is excluded that nonetheless can cause high risks to individuals (Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet, 2013; 6).

The Dutch Data Protection Authority has published policy rules regarding the data breach notification obligation as laid down in the Dutch Data Protection Act (Dutch Data Protection Authority, 2015). According to the policy rules the *nature of the affected data* is relevant when deciding whether there is

[9] https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

a considerable likelihood of serious adverse effects (Tweede Kamer, 2015; 24). This means that breaches that encompass sensitive personal data such as special personal data as referred to in article 16 of the Dutch Data Protection Act, data about the financial or economic situation of the data subject and (other) data that may lead to stigmatisation or exclusion of the person involved (such as gambling addiction, school performance or relational problems), must be notified.

Also the *nature and extent of the affected processing* helps to determine the answer to the question whether the data breach leads to a considerable likelihood of adverse effects on the protection of personal data. A data breach at organisations such as the Tax Office, the Social Insurance Bank or at a commercial bank or insurer may lead to financial damage for the data subject (Wijziging Wet bescherming persoonsgegevens, 2013; 7). Security flaws in the processing of personal data held by public authorities may also have severe consequences for those involved (Wijziging Wet bescherming persoonsgegevens, 2013; 20). The extent of the processing means that data breaches may involve many personal data per person, or data from large groups of data subjects. Data processing operations by the government can also involve personal data that are shared within chains; loss or compromised personal data may affect the entire chain. This will increase the risk to the rights and freedoms of data subjects.

Except for the nature of the affected data and the nature and extent of the affected processing, parliamentary history in the Netherlands also draws attention to the position of vulnerable groups (Tweede Kamer, 2015;24)(Dutch Data Protection Authority, 2015; 28). For data subjects in vulnerable groups, loss or unlawful processing of personal data may cause additional risks. For certain categories of data subjects, such as children or people with intellectual disabilities, it may be more difficult to deal adequately with the consequences of a personal data breach. For example, they might be more likely to become the victim of phishing because they will have more problems to distinguish genuine mails from fake electronic mails.

Article 34a, paragraph of the Dutch Data Protection Act stipulates that if the controller has taken adequate protection measures to render the relevant personal data incomprehensible or inaccessible to anyone who has no right to take knowledge of that information (for instance adequate encryption), there is no obligation to notify the supervisory authority and to inform the data subject *if a back-up of the personal data is available*. In this situation there is no personal data breach because no personal data has been lost and it reasonably can be excluded that personal data have been processed unlawfully. However encrypted devices (e.g. laptops) that are stolen and that contain personal data, have to be notified to the supervisory authority and to the data subjects if there is *no* back-up available. It will have adverse effects, because the personal data will have to be provided again by the affected individuals (Dutch Data Protection Authority, 2015; 25, 34, 39). Despite the limited negative consequences for the data subjects, the latter must be informed of the data breach (Dutch Data Protection Authority, 2015; 39)(Article 29 Data Protection Working Party, 2014b, case 5). Adequate protection measures such as encryption, hashing and remote wiping therefore can be applied to prevent notification of personal data breaches to the supervisory authorities and data subjects (in

cases when a back-up is available). To assess whether protection measures such as encryption and hashing are adequate, the quality of the algorithm, the strength of the decryption key, the irreversibility of the encryption and the non repeatability of the hash key are relevant conditions (Dutch Data Protection Authority, 2015; 36).

The Dutch Minister for Security and Justice also has stated that technical security (protection) measures, the scope and extent of the personal data breach and the sensitivity of the personal data determine whether there is a serious adverse effect on the protection of personal data (Tweede Kamer, 2015; 25).

4.3.5. Risk and high risk in the GDPR

As highlighted in chapter 3, the notion of risk and high risk has been introduced in the GDPR. High risk processing activities as included in article 35, paragraph 3 of the GDPR for which a data protection impact assessment should be required, refers to (quote):

- *'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*

- *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*

- *a systematic monitoring of a publicly accessible area on a large scale.'*

High risk therefore includes a combination of profiling activities, large scale use of new technology, large scale processing of sensitive personal data as defined by article 9 and 10 GDPR and large scale (systematic) monitoring of publicly accessible areas.

It is likely that the Article 29 Data Protection Working Party will give a more detailed definition and overview of processing activities that should be considered to be high risk to the rights and freedoms of data subjects. The notion of high risk and data protection impact assessment is included in the 2016 Action Plan of the Article 29 Data Protection Working Party for the implementation of the GDPR (Article 29 Data Protection Working Party, 2016b; 2). The Centre for Information Policy Leadership (CIPL), a London based think tank, already has published various papers that discussed the risk-based approach in the data protection domain (2014a, 2014b, 2014c, 2016a, 2016b). The most recent CIPL paper contained an overview of examples, criteria and/or characteristics of high risk data processing (CIPL, 2016b). This overview is presented in Figure 3 on the next page.

	Examples, Criteria and/or Characteristics of "High Risk"
1	Scope of material and non- material damage (e.g. individual, population of relevant individuals or society generally)
2	Impact of material and non- material damage (e.g. individual, population of relevant individuals or society generally)
3	Volume of personal data processed
4	Number of data subjects
5	The number of parties (e.g. third-parties and employees) accessing the data
6	The type and number of third-party recipients
7	Geographical spread of processing activities
8	Processing multiple data sources
9	Type of personal data processed – e.g. sensitive personal data, or personal data regulated by other laws (health, financial, biometrics)
10	Length of data processing
11	Processing of data collected from individuals ("original" personal data) or data derived, observed, inferred about individuals ("secondary" personal data)

Figure 3: Examples, criteria and/or characteristics of 'High Risk' data processing (CIPL, 2016b; 26-27)

The GDPR only refers to risks and high risks, no reference is made to low risks or no-risk categories of processing activities. However, one could argue that the GDPR makes implicit suggestions for low-risk or no-risk categories as well, because article 30, paragraph 5 of the GDPR lifts an enterprise or organization with fewer than 250 employees from the obligation to maintain records regarding data processing, unless (quote): *'the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10'* (Article 30, paragraph 5 GDPR) (See also Schwarz, 2016). Article 35, paragraph 5 of the GDPR also permits data protection authorities in Europe to establish lists of processing operations that do not require data protection impact assessments (CIPL, 2016b; 15). As data protection impact assessments are only mandatory for high risk processing operations, such an exemption list should include an overview of risk, low risk or no risk processing operations.

4.3.6. Personal data and risk classification

In 2001 the Dutch Data Protection Authority has published a background study on the protection of personal data (Blarkom and Borking, 2001). The intention of the background study was to give guidance regarding the security measures that should be taken to protect different categories of personal data. This 'security' obligation is included in article 13 of the Dutch Data Protection Act that is based on article 17 ('Security of Processing') of the Data Protection Directive 95/46/EC. Article 17 of

the European Data Protection Directive 95/46/EC states (quote): *'(....) that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'* Article 13 of the Dutch Data Protection Act and Article 32 of the GDPR contain similar provisions for the security of processing.

The background study of the Dutch Data Protection Authority of 2001 includes in paragraph 3.3 a risk-classification of processing of personal data ('risicoklassen'). Security measures have to be implemented that are proportional to the risk-level of each risk classes. The risk-classification contains four classes: risk class 0 (public data), risk class I (basic level), risk class II (increased risk) and risk class III (high risk). The risk class 0 contains personal data that do no cause risks to the affected data subjects. Examples that are included in this risk class are public telephone directories, public brochures and public websites. The personal data that are included in this risk class do not need additional security measures. Risk class I (basic level) contains personal data that are sufficiently protected by standard (information) security measures. Examples of personal data that are included in this risk class are subscriptions, labor relations, customer relations and similar relations between a data subject and an organization. These are personal data such as name and address for education (school), rent of an apartment, hotel guests and members of an organizations or subscriptions to a newspaper. The third risk class (risk class II) can be defined as 'increased risk' and contains sensitive personal data such as gender, political preference, race, personal data that contains the processing of bank and insurance accounts that indicates the personal or economic situation of the data subject, credit information or debt restructuring or repayment, personal data that relates to the whole population or large parts of the population (even if it comprises basic personal data) and all other processing of personal data that is similar to the earlier categories that are mentioned. Compared to the risk class I (basic level), higher norms for security measures have to be implemented for the risk class II (increased risk), taken into consideration the additional negative consequences that will occur by loss, inaccurate and inadequate processing of these personal data. The final risk class III (high risk) contains the processing of personal data by surveillance authorities with special authorization and processing that can seriously affect the interests of data subjects when processing takes place inaccurate or unauthorized. Special processing activities are included in this last category, such as the processing of DNA of data subjects. Also processing of personal data that is subject to oaths of secrecy fall within this risk class III category. Personal data that is included in this risk class III (high risk) category, should be flagged with a visible marker on the data carriers such as an USB-stick, CD ROM etc.

The Dutch Data Protection Authority has drafted the following figure to indicate the relationship between the four risk classes (see next page):

Nature of the personal data		Personal data	Sensitive personal data	Financial and/or economic personal data
Number of personal data (nature and amount)	Nature of the processing			
Small amount of personal data	Low complexity of processing	**Risk class 0**	**Risk class II**	**Risk class II**
High amount of personal data	High complexity of processing	**Risk class I**	**Risk class III**	

Figure 4: Risk classes of processing of personal data (Blarkom and Borking, 2001; 29)

4.3.7. Incident reporting in the NIS-Directive

The Directive on security of network and information systems (NIS Directive, 2016) includes a legal obligation both for operators of essential services (article 14) and digital service providers (article 16) to report incidents. Incidents are defined as (quote): *'any event having an actual adverse effect on the security of network and information systems'* (NIS Directive, article 4, paragraph 1, under 7). Such incidents can also relate to personal data. Recital 63 of the NIS Directive states that (quote): *'personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents.'* Article 14 stipulates that operators of essential services have to notify, with undue delay, the competent authority or the Computer Security Incident Response Team (CSIRT) of incidents having a significant impact on the continuity of the essential services they provide. Types of entities that can be considered to be operators of essential services are included in Annex II of the NIS-Directive such as oil, gas, electricity, water transport, road transport, banking and digital infrastructure. Article 16 includes an obligation for digital service providers to notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of online marketplaces, online search engines and cloud computing services. Digital service provider means any legal person that provides a digital service such as online marketplaces, online search engines and cloud computing services (NIS-Directive, article 4, paragraph 5 and 6). The Directive has been published in the Official Journal of the European Union on 19th July 2016 (OJ L 194, 19.7.2016, p. 1–30) and will have to be implemented in EU Member States within 21 months after publication.

The incident reporting obligations of the NIS-Directive contain a similar risk-based threshold compared to the personal data breach notification that is included in the GDPR. Incidents within the NIS-Directive only have to be reported to the competent authority or CSIRT if these incidents have *significant* impact on the continuity of essential services, or have *substantial* impact on the provision of digital services. The criteria that have to be applied to determine the significance of the impact of an incident on the continuity of essential services, are included in article 14, paragraph 4 of the NIS-Directive. These are

(quote): *'(a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident'*. Article 16, paragraph 4 contains the criteria that should be applied to determine whether the impact of an incident is substantial for the provision of online marketplaces, online search engines and cloud computing services. These are (quote): *'(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent of the disruption of the functioning of the service; (e) the extent of the impact on economic and societal activities'.*

A final remark can be made about the Dutch legislative proposal for Data Processing and Cyber Security Breach Notification (Wet gegevensverwerking en meldplicht cybersecurity, 2016) which includes an obligation for operators of essential (vital) services to notify security and integrity breaches of information systems that result or can result in a significant disruption of the availability and reliability of a service or product. This proposal has been submitted to the Dutch Parliament in anticipation of the NIS-Directive, and will probably enter into force in 2017. The notification obligation will only apply for suppliers of essential (vital) services such as electricity, gas, drinking water, telecom, financial sector government, transport and the nuclear sector. The exact meaning of 'significant disruption' will be debated with the various stakeholders and may include measurable thresholds that will be published for each product and service. Criteria that can be applied are for instance the duration, severity and scale of the disruption (Wet gegevensverwerking en meldplicht cybersecurity, 2016, nr 3; 4, 28), but also the number of people that is affected (Wet gegevensverwerking en meldplicht cybersecurity, 2016, nr 6; 8).

4.4. Construction of a privacy risk classification framework

This chapter has dealt with the construction of a privacy risk framework for personal data breach notifications. The purpose of such privacy risk classification framework would be to rate risks to the rights and freedoms of the data subject that are caused by personal data breaches and ultimately, to create a privacy risk classification framework that includes risks and high risks, but even so low risks and no risks.

Some authors and institutions have published guidelines about (qualitative) criteria that could be applied to monitor whether personal data breaches should be notified to the supervisory authority and communicated to the data subjects. ENISA (2011) for instance refers to the number of people that are affected, nature of the data that has been affected (financial, health, etc.), nature of the breach (widespread, or an isolated incident) and the security level (has the data been encrypted). In its report on recommendations on technical implementation guidelines for personal data breach notifications, ENISA (2012) referred to the criteria of 'identifiability of data' and 'level of exposure' to determine the impact of the data breaches on individuals; this included amongst others the sensitivity of personal data, the type of the breach and the delay to identify the breach. Also Etzioni (2013, 2015b) proposes a framework that is based on volume, sensitivity of data and cybernation to indicate when processing of data causes specific risks to the privacy of individuals. The Dutch Data Protection Authority (2015)

stresses the nature of the affected data (e.g. sensitive personal data) and the nature and extent of the affected processing (e.g. large scale data processing and data chain effect) as well as the position of vulnerable groups and adequate protection measures (such as encryption, remote wiping, hashing etc.) as criteria for the risks to the rights and freedoms of data subjects caused by a personal data breach. Also some other countries such as Austria (2010), Germany (2009), Ireland (2011) and Canada (2014) apply similar risk thresholds for the notification of personal data breaches. The concept of high risk data processing activities as defined in the GDPR focuses on large-scale operations, sensitivity of data, new technologies, profiling and large scale monitoring of publicly accessible areas (GDPR, article 35). Finally the background study of the Dutch Data Protection Authority (Blarkom and Borking, 2001) referred to the sensitivity of personal data, the degree of complexity of processing (low/high) and the amount of personal data that is involved in the processing to determine four risk-classes.

Based on these findings, the key criteria that should be applied to construct a privacy classification framework for personal data breaches, center around:

- The sensitivity of the personal data. In case of personal data breaches that involve sensitive personal data (such as health related or financial personal data), there will be high risks for the rights and freedoms of data subjects.

- The scale of operations. In case of large scale operations that involve a large number of people, large volume of personal data items and include data chain effects (cybernation) and profiling, there will be high risks for the rights and freedoms of data subjects in case of personal data breaches.

- The presence of adequate security measures to protect and/or anonymize personal data such as encryption, pseudonymization, remote wiping, hashing of personal data, access management etc. If such adequate security measures are in place and there is a back-up available of the personal data that has been rendered incomprehensible or inaccessible, the risks for the rights and freedoms of data subjects in case of personal data breaches will be absent.

In addition to these criteria, the incident reporting as included in the NIS-Directive refers to the *geographical spread* and *duration* of the incident as relevant criteria in the context of personal data breach notifications. Another criterion that could play a role, is whether the data processing has an *occasional* or *structural* character. The criterion of processing being ‘occasional’ for instance is applied in article 30 GDPR to exempt organisations employing fewer than 250 persons from keeping records of processing activities. This argument is also included in the monetary penalty notice of the Information Commissioner’s Office (ICO) that has been issued to TalkTalk as follow-up to the personal data breach that took place in 2015 (ICO, 2016). ICO took into consideration whether the breach could be characterized as one-off (‘occasional’) event and attributable to human error as eased circumstances. This was not the case as TalkTalk had failed to remove, or make secure, the

webpages that enabled the attackers to access the underlying database. As consequence ICO issued its biggest ever fine of £ 400.000 to TalkTalk.[10]

The criteria that have been discussed in this paragraph can be bundled in three categories, i.e. criteria that relate first to the *nature of the affected data* (such as sensitive or no-sensitive personal data), second to the *nature and extent of the affected processing* (such as number of data subjects affected, cybernation, geographical spread, profiling, (non) structural character of breach and duration of breach) and third to adequate *security measures* to protect the personal data (such as encryption or remote wiping). A heat map can be drafted to construct a visual representation of the privacy risk classification framework for personal data breach notifications (Figure 5). The green area highlights the area where the risks to the rights and freedoms of data subjects, i.e. the respect for private and family life and the protection of personal data, as result of the personal data breach are absent or limited, for instance due to the fact that only stand-alone non-sensitive personal is breached for a short duration, in a small geographical area with an occasional character and adequate security measures in place. The red area indicates the high risk area for personal data breaches, for instance large scale data processing (i.e. large number of data subjects and large geographical area) that includes sensitive data and profiling, with a long duration of the personal data breach and without any adequate security measures in place.

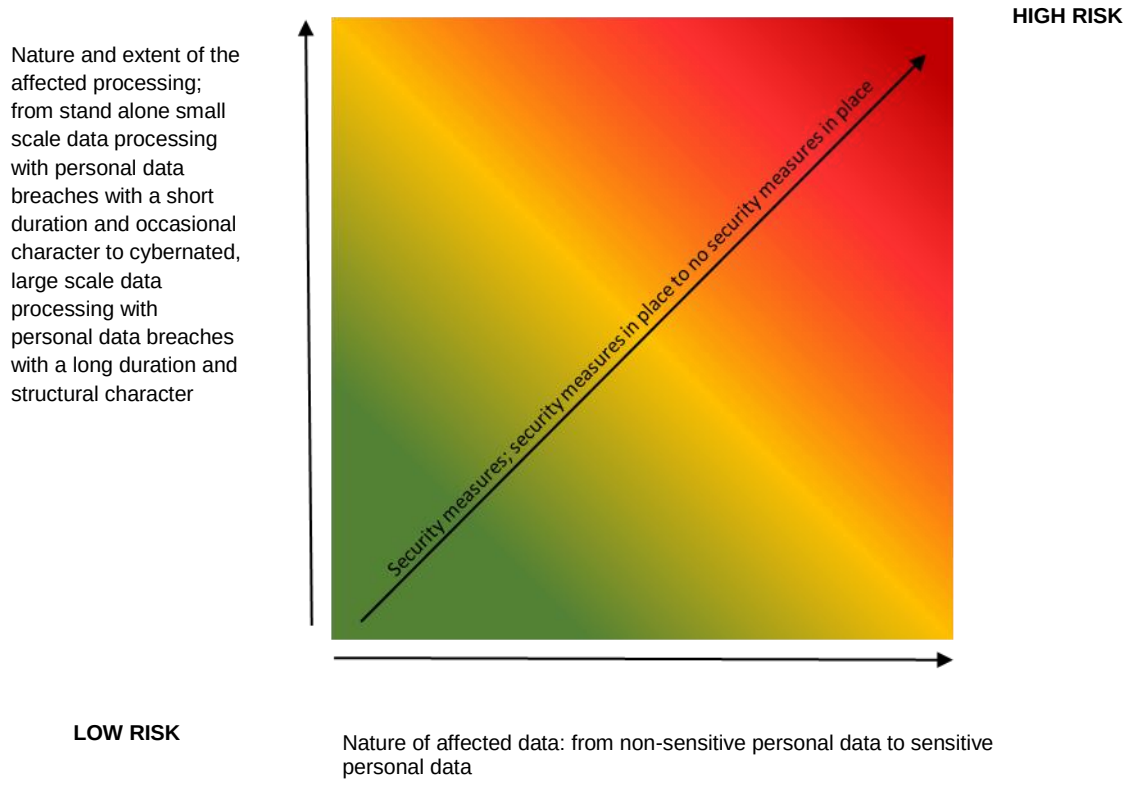


Figure 5: Heat map as visualization of the privacy risk classification framework for personal data breach notifications

[10] Information Commissioner's Office (ICO), "TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack", 5 October 2016, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

It seems difficult to construct a privacy risk classification framework that is based on *quantitative* criteria because the exact demarcation will depend on the context of each specific personal data breach. Some stakeholders however have proposed specific numbers related to risks relating to processing of personal data. The European Parliament for instance has considered processing operations relating to more than 5000 data subjects during any consecutive 12-month period as likely to present specific risks (LIBE Committee, 2013). In California, Alaska and Hawaii disclosure to the authorities only applies when the breach affects more than a certain number of individuals, e.g. 500 in California, or 1,000 in Alaska and Hawaii (Tana, 2013). Personal data breaches in Ireland do not have to be notified to the Data Protection Commissioner if the breach does not affect more than 100 data subjects (Hallinan, 2011). The method that offers the most potential to construct a privacy risk classification framework for personal data breach notifications based on *quantitative* criteria (i.e. a semi-quantitative analysis), is developed by ENISA (2012) for providers of publicly available electronic communications services. The method proposed by ENISA – and also applied by CNIL – however has a particular focus on the impact or the 'adverse effect' on the individuals whose personal data have been breached and not on the likelihood of personal data breaches.

4.5. Conclusion

Building blocks for the construction of a privacy risk classification framework for personal data breach notifications in the GDPR can be found in publications of ENISA (2011)(2012), Etzioni (2015b), the German (2009), Canadian (2014), Austrian (2010) and the Dutch Data Protection Act (2015), the Irish Personal Data Security Breach Code of Practice (2011), background study and guidelines of the Dutch Data Protection Authority (2001)(2015) and publications of the Centre of Information Policy Leadership (2014a, 2014b, 2014c, 2016a, 2016b). All these sources have in common that they center around three categories of qualitative criteria that determine the risk to the rights and freedoms of data subjects relating to personal data breaches, i.e. criteria that relate first to the *nature of the affected data* (such as sensitive or no-sensitive personal data), second to the *nature and extent of the affected processing* (such as number of data subjects affected, cybernation, geographical spread, profiling, (non) structural character of breach and duration of breach) and third to adequate *security measures* to protect the personal data and mitigate the impact of personal data breaches (such as encryption or remote wiping).

Chapter 5: De minimis rule for personal data breach notifications

5.1. Online questionnaire de minimis rule

To assess the feasibility of a de minimis rule for personal data breach notifications, an online questionnaire has been drafted. The online questionnaire has been sent to members of the Privacy Commission of the Confederation of Netherlands Industry and Employers (known as VNO-NCW), being the largest employers' organization in the Netherlands, to the members of the Regulatory Affairs Commission of the Dutch Data Driven Marketing Association and to the members of the risk subgroup of the Centre for Information Policy Leadership (CIPL). This risk sub group is set-up to assist companies to implement the GDPR. Together they represent the views of privacy and security professionals that are employed by private companies in the Netherlands and Europe. The findings of the questionnaire and the draft version of the thesis have been discussed at the risk workshop of CIPL that was organized on 19th and 20 September 2016 in Paris as part of the GDPR Implementation Workshop of CIPL. Also some other privacy and security experts have been consulted, such as academics and government officials. A copy of the questionnaire and the aggregated responses has been attached as annex to the thesis.

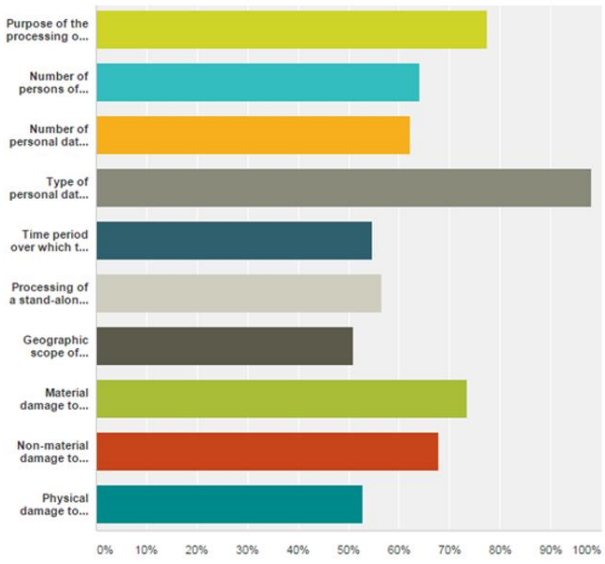
In total 55 national and international privacy and security experts have responded to the questionnaire from the 4th of August until the 15th September 2016. Of the 55 respondents 39 are employed in the private sector, 6 in the academic sector, 3 in the government and 3 in the non-profit sector (4 persons skipped the question). Of these 55 persons, 20 are data protection officers, 10 are legal counsels (other than data protection officer), 7 are consultants, 4 are security officers, 4 are (assistant) professors, 2 are compliance managers, 1 trade association representative and 1 engineer (6 persons skipped the question). 41 persons are based in the Netherlands; 12 respondents are based outside the Netherlands of which 2 in the United States of America and 10 in EU Members States (UK, France, Belgium and Switzerland)(2 persons skipped the question).

The first question related to the sources that can be used to formulate a framework for a risk-based approach in the data protection domain. Most respondents (39 (73.58%) of the 53 respondents) referred to privacy impact assessments as main source, followed by personal data breach notification guidelines (34 (64.15%)), national data protection laws that already include a personal data breach notification obligation (31 (58.49%)), data protection impact assessments (RFID, Smart Meters)(26 (49.06%)) and privacy risk management guidelines (CINL, NIST)(24 (45.28%)). Sources that relate to cyber security publications such as cyber security risk assessments (14 (26.42%)), national (cyber) security laws (21 (39.62%)) and reports of ENISA (21 (39.62%)) scored a little bit lower. Some individual respondents also referred to decisions of data protection authorities and courts, business continuity risk management publications and opinions of the Article 29 Data Protection Working Party.

A majority of the respondents (29 (65.91%)) stated that a distinction between vulnerable groups of people (such as elderly people or disabled people) and non-vulnerable groups of people cannot be used to formulate a de minimis rule for personal data breach notifications. This seems to contradict the

view of the Dutch Parliament that stated that vulnerable groups of people should be taken into account in the context of a personal data breach notification (Tweede Kamer, 2015;24)(Dutch Data Protection Authority, 2015; 28). However, the presumption that it seems sensible to make a distinction between vulnerable and non-vulnerable groups of people when dealing with personal data breaches, does not mean that the same distinction is relevant for the formulation of a de minimis rule. Therefore, the majority of the respondents are right to dismiss this criterion for the construction of a de minimis rule. A majority of the respondents (35 (77.78%)) stated that a de minimis rule can also be applied to other articles of the GDPR that includes a risk-based approach such as for instance the data protection impact assessment (article 35 GDPR).

According to the GDPR the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing (GDPR, 2016, recital 76). The criteria, and the scores of the respondents, that can be applied to identify and measure the nature, scope, context and purpose of the processing are shown in Figure 6. Most respondents (52 (96,11% of the 53 respondents) indicated that the type of personal data (sensitive/ non-sensitive) that will be processed, is the most important criterion for any privacy risk assessment.



Answer Choices	Responses
Purpose of the processing of personal data	77.36% 41
Number of persons of which personal data will be processed	64.15% 34
Number of personal data items that will be processed (for instance name, address etc)	62.26% 33
Type of personal data (sensitive/ non-sensitive personal data) that will be processed	98.11% 52
Time period over which the personal data will be collected and retained	54.72% 29
Processing of a stand-alone personal data set in combination with other personal data sets (data chain effect)	56.60% 30
Geographic scope of personal data that will be processed	50.94% 27
Material damage to natural persons that is caused by the privacy infringement	73.58% 39
Non-material damage to natural persons that is caused by the privacy infringement	67.92% 36
Physical damage to natural persons that is caused by the privacy infringement	52.83% 28

Figure 6: Criteria that can be applied to identify and measure the nature, scope, context and purpose of the processing (53 respondents).

The question, and scores of respondents, whether these criteria can be applied to formulate a de minimis rule for personal data breach notifications is depicted in Figure 7 ('Do you think (the criterion) can be used to formulate a de minimis rule for personal data breach notifications?'). From this figure the conclusion can be drawn that especially the *type of personal data* is considered by the respondents to be an important criterion to define a de minimis rule for personal data breach notifications (44 respondents state 'yes', 93.62%), followed by the material and non-material damage to natural persons that is caused by the personal data breach (30 (65.22%)), (30 (65.22%)), the nature of personal data breaches (27 (60%)), purpose of processing of personal data (29 (55.77%)), the

number of personal data items that will be processed (for instance name, address etc) (28 (54.90%)) and the number of persons of which personal data will be processed (27 (51.92%)). Also the processing of a stand-alone personal data set in combination with other personal data sets (data chain effect) has a relative high score as criterion that can be applied to formulate a de minimis rule for personal data breach notifications (24 (52.17%)).

	Yes	No	No Opinion
Purpose of the processing of personal data	29 (55.77%)	16 (30.77%)	7 (13.46%)
Number of persons of which personal data will be processed	27 (51.92%)	23 (44.23%)	2 (3.85%)
Number of personal data items that will be processed (for instance name, address etc)	28 (54.90%)	20 (39.22%)	3 (5.88%)
Type of personal data (sensitive/ non-sensitive personal data) that will be processed	44 (93.62%)	3 (6.38%)	0 (0.00%)
Time period over which the personal data will be collected and retained	19 (40.43%)	25 (53.19%)	3 (6.38%)
Processing of a stand-alone personal data set in combination with other personal data sets (data chain effect)	24 (52.17%)	16 (34.78%)	6 (13.04%)
Geographic scope of personal data that will be processed	17 (36.96%)	28 (60.87%)	1 (2.17%)
Material damage to natural persons that is caused by the privacy infringement	30 (65.22%)	15 (32.61%)	1 (2.17%)
Non-material damage to natural persons that is caused by the privacy infringement	30 (65.22%)	16 (34.78%)	0 (0.00%)
Physical damage to natural persons that is caused by the privacy infringement	19 (42.22%)	19 (42.22%)	7 (15.56%)
Nature of personal data breaches (e.g. copying, removal or destruction, theft etc)	27 (60%)	17 (37.78)	1 (2.22%)

Figure 7: Criteria that can be applied to formulate a de minimis rule for personal data breach notifications; scores of respondents (yes/no/ no opinion) (number of respondents and percentage)

The next step is to investigate what kind of data categorization can be applied for each of those criteria and whether quantative thresholds can be used to define a de minimis rule for personal data breach notifications. Only those criteria for which a majority of the respondents (> 50%) indicated that it can be used to formulate a de minimis rule for personal data breach notifications, will be taken into account. Criteria that score lower (<) than 50% on the `yes` in Figure 7 will be left aside. This means that the time period over which the personal data will be collected and retained, i.e. personal data is collected real time, for one day, for one month, for six months, for one year or for more than one year, will not be taken into consideration to formulate a de minimis rule for personal data breach notifications; only 19 (40.43%) of the 47 respondents considered this criterion as relevant for a de minimis rule. The same accounts for the geographical scope of the personal data that will be processed (17 (36.96%) of 46 respondents found this criterion relevant) and the physical damage to natural persons that is caused by the personal data breach (19 (42.22%) of 45 respondents found this criterion relevant).

5.2. Building blocks for a de minimis rule

In this paragraph the criteria that have been indicated by a majority of the respondents (> 50%) to be relevant for the formulation of a de minimis rule for personal data breach notifications, will be discussed. The building blocks for the formulation of a privacy risk classification framework that has been discussed in the previous chapter will also be used to support the construction of a de minimis rule.

5.2.1. Type of personal data

The online questionnaire included a vast range of examples of types of data that could be included in a de minimis rule for personal data breach notifications, ranging from name, address and telephone number of the data subject to health and medical data, sexual orientation and religious beliefs. As stated before, a majority of the respondents (44 (93.62%) of total 47 responses) indicated that type of personal data can be applied to formulate a de minimis rule for personal data breach notifications. However, the responses did not present a clear picture about the specific types of personal data (e.g. names, addresses, telephone numbers etc.) that should be included in a de minimis rule. The building blocks for a privacy risk classification framework that have been identified in the previous chapter, however do offer some insights.

Legislation (Germany, 2009)(Dutch Data Protection Act, 2015)(Canada, 2014)(Ireland, 2011) and guidelines regarding data protection and personal data breach notification (ENISA, 2012)(CIPL, 2016b)(Dutch Data Protection Authority, 2015)(Blarkom and Borking, 2001) all state that the type of personal data can be classified according to the sensitivity of the personal data. This means that breaches that encompass sensitive personal data such as special personal data as referred to in article 16 Dutch Data Protection Act, Article 9 and 10 of the GDPR, data about the financial or economic situation of the data subject and (other) data that may lead to stigmatisation or exclusion of the person involved, must be notified. According to Article 9 of the GDPR, special categories of personal data include processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. The classification of types of personal data that has been applied by the Dutch Data Protection Authority (Blarkom and Borking, 2001; 26-28) seems to offer the most useful framework. This means that a classification of public data (risk class 0), basic level of personal data (risk class I), increased risk of personal data (risk class II) and high risk of personal data (risk class III) is the most appropriate. As the risk class 0 contains personal data that does not cause risks to the affected data subjects, such as public telephone directories, public brochures and public websites, personal data breaches that only include personal data of risk class 0 do not have to be notified to the supervisory authority (or communicated to the individual data subject who is affected).

5.2.2. Material and non-material damage to natural persons

As stated before, 30 (65.22%) of the 46 respondents have indicated that material damage is a relevant criterion to formulate a de minimis rule for personal data breach notifications. For material damage that is inflicted upon data subjects as a consequence of personal data breaches, a classification has been made in the online questionnaire between material damage of less than € 100 per data subject, less than € 200, less than € 300, less than € 400, less than € 500 and less than € 1000. 3 (12.5%) of the 24 respondents to the online questionnaire indicated that material damage of less than € 100 should be part of a de minimis rule, while 3 (12.5%) stated that a material damage of less than € 200 should be part of a de minimis rule. 17 respondents (70.8%) stated that the monetary value of the material damage depended on the personal data breach and its specific context. 1 respondent (4.17%) indicated that material damage of less than €1000 should be part of a de minimis rule. Within the data protection domain there is no information available that indicates what monetary value can be applied as 'material' threshold to measure whether a personal data breach is deemed to have a impact that result in a risk to the rights and freedoms of data subjects.

However the European Convention on Human Rights (ECHR) offers some guidance on this criterion. Paragraph 1 of article 8 of the ECHR ('Right to respect for private and family life') states that (quote): *'Everyone has the right to respect for his private and family life, his home and his correspondence.'* The ECHR contains in article 35, paragraph 3 a de minimis rule for applications that are submitted by persons, non-governmental organizations or group of individuals claiming to be the victim of a violation of the rights that are included in the ECHR (Council of Europe, 2004). In 2010 article 35, paragraph 3, under b) of the ECHR has entered into force, according to which the Court shall declare inadmissible any individual application if (quote): *'(...) the applicant has not suffered a significant disadvantage (...)'*. The European Court of Human Rights has evaluated article 35, paragraph 3 under b) in 2012 (European Court of Human Rights, 2012). Based on decisions that has been published by the European Court of Human Rights since the entering into force of this criterion, it concludes that as far as insignificant financial impact is concerned, the Court has found a lack of significant disadvantage (quote*): 'where the amount in question was equal or inferior to roughly EURO 500.'* (European Court of Human Rights, 2012; 5). This would imply that a de minimis threshold for material (e.g. financial) damage as a consequence of a personal data breach would be around € 500 per individual person.

Although only 19 (42.22%) of the 45 respondents stated that physical damage is a relevant criterion for the formulation of a de minimis rule for personal data breach notifications and therefore scores below 50%, it will be shortly discussed because it can be considered to be a subset of the criterion of material damage. Only 15 respondents (27.2%) of the 55 participants to the online questionnaire gave input on the open question what kind of types of physical damage should be considered to be relevant to formulate a de minimis rule for personal data breach notifications (no standard suggestions were given in the questionnaire); answers ranged from physical damage to fear, psychological stress and domestic abuse and injuries. Some also stated that it depended on the specific case and its sensitivity.

Therefore, based on the results of the online questionnaire, its seems not possible to formulate a de minimis rule for physical damage as a result of a personal data breach.

Although 30 (65.22%) of the 46 respondents have indicated that non-material damage is a relevant criterion to formulate a de minimis rule for personal data breach notifications, it seems difficult to formulate a de minimis rule for non-material damage that is inflicted upon the rights and freedoms of data subjects as a consequence of personal data breaches. Non-material damage categories that are mentioned by respondents in the online questionnaire are: loss of control over personal data, discrimination, identity theft, fraud, damage to reputation, loss of confidentiality of personal data and unauthorized reversal of pseudonymisation. None of these categories scored extremely high as indicator of a de minimis rule for personal data breach notification. 25 (75.76%) of the 33 respondents indicated that the relevant non-material damage categorization depends on the personal data breach and its specific context. Based on the evaluation of the way the de minimis rule of article 35, paragraph 3 under b) of the ECHR has been applied regarding the threshold of non-financial damage (i.e. whether the applicant has suffered a significant non-financial disadvantage), the European Court of Human Rights mainly refers to court cases, the length of prison sentences and the circumstances under which employees were fired (European Court of Human Rights, 2012; 7). This evaluation however does not give any guidance to the way the criterion of non-material or non-financial damage can be applied to formulate a de minimis rule for personal data breach notifications.

5.2.3. Purpose of processing of personal data

29 (55.77%) of the 52 respondents indicated that the purpose of processing of personal data is a relevant criterion for the formulation of a de minimis rule for personal data breach notifications. Regarding the follow-up question (‘what categorization for the purpose of processing of personal data can be formulated as part of a de minimis rule for personal data breach notifications?’) a fierce majority of the respondents (27 (81.82%) of the 33 respondents) indicated that it depends on the personal data breach and its specific context. However 11 respondents (33.33%) of the respondents also indicated that billing and collection should be part of a de minimis rule, 6 (18.18%) referred to direct marketing, 5 (15.15%) referred to (online) purchases and 12 (36.36%) referred to profiling as part of de minimis rule for personal data breach notifications. Therefore the results of the online questionnaire do not present a clear picture what kind of purposes of processing of personal data can be used to formulate a de minimis rule for personal data breach notifications.

5.2.4. Number of persons and number of personal data items

28 (54.90%) of the 51 respondents indicated that the number of personal data items should be applied to formulate a de minimis rule for personal data breach notifications, while 27 (51.92%) of the 52 respondents indicated the same for the number of persons. Regarding the follow-up question (‘what categorization should be applied as part of the quantitative threshold for the number of personal data items?’) 19 (73.08%) of the 26 respondents indicated that the number of personal data items that should be part of a de minimis rule depended on the personal data breach and its specific context, while 3 (11.54%) respondents stated that one personal data item should be part of de minimis rule; 3

(11.54%) respondents indicated that more than 5 personal data items should be part of such a rule and 1 respondent (3.85%) indicated that processing of (1-5) personal data items should be part of de minimis rule. One of the respondents stated in the comments that (quote): *'It is highly unlikely that you process less than 5 personal data items of someone, especially if you also take online identifiers into account'.* Regarding the number of persons, 18 (72%) of the 25 respondents stated that the number of persons that should be part of a de minimis rule depended on the personal data breach and its specific context, while 4 (16%) respondents indicated that processing of personal data of one person should be part of de minimis rule. 3 (12%) respondents indicated that processing of personal data of more than one person should be part of de minimis rule.

Based on the results of the online questionnaire, it seems that a de minimis threshold for the number of personal data items and number of persons is difficult to formulate. As one of the respondent has stated (quote): *'a usbstick with 10 addresses is not very exciting, a usbstick with 10 addresses marked as HIV infected person is a severe data breach, so it is about context.'* Also the Article 29 Data Protection Working Party has stated that personal data breaches should be notified, independently to the number of data subjects concerned (Article 29 Data Protection Working Party, 2012). ENISA has stated that the number of people by the personal data breach should not be used as a criterion for assessing the impact of the personal data breach (ENISA, 2012; 25). These comments however have been made with regards to the mandatory personal data breach notification that is included in the revised e-Privacy Directive (Directive 2009/136/EC, 2009). The personal data breach notification that is included in that Directive does not include a risk-threshold for notification and for which the European Commission has stated that *all* personal data breaches should be notified to the competent national authority and that no discretion should be left to the provider whether or not to notify (European Commission, 2013; recital 6). As stated in the previous chapter, the number of persons that are affected by the personal data breach and the number of personal data items involved, have found to be relevant criteria by various sources to be able to assess the risk that is imposed upon the rights and freedoms of the data subjects as consequence of a personal data breach (Etzioni, 2015b)(CIPL, 2016b)(Blarkom and Borking, 2001)(Dutch DPA, 2015). Some national laws even include a threshold for personal data breach notification to the supervisory authorities. For instance the Personal Data Security Breach Code of Practice in Ireland prescribes that personal data breaches do not have to be notified to the Data Protection Commissioner if the breach is notified promptly to data subjects, it does not include sensitive or financial data and the breach does not affect more than 100 data subjects (Hallinan, 2011). Also in California, Alaska and Hawaii notification of personal data breaches only applies when the breach affects more than 500 individuals in California and 1000 individuals in Alaska and Hawaii (Tana, 2013). Last but not least, the European Parliament has defined specific risks as processing of personal data relating to more than 5000 data subjects during a 12-month period (LIBE Committee, 2013).Various laws therefore apply different notification-thresholds for the number of persons that are affected by the personal data breach. There is no 'one size fits all'. The conclusion therefore should be that the number of personal data items and number of persons that are affected by a personal data breach, cannot be applied as a criterion to formulate a de minimis rule for personal data breach notifications.

5.2.5. Nature of personal data breaches

27 (60%) of the 45 respondents stated that the nature of personal data breaches (e.g. copying, removal or destruction, theft etc.) can be used to formulate a de minimis rule for personal data breach notifications. In answer to the follow-up question what categories ('nature') of personal data breaches can be formulated as part of a de minimis rule for personal data breach notifications, 24 (82.76%) of the respondents stated that such categories depend on the personal data breach and its specific context. Also most of the sources that have been identified in chapter 4 for the formulation of a privacy risk classification framework do not give any insights into the use of the nature of personal data breaches for the construction of a de minimis rule. The only exception is ENISA (2012) which pinpoints to the nature of the breach and type of exposure as one of the criteria to determine the level of exposure that is accomplished by the personal data breach. Regarding the nature of the breach/ level of exposure, ENISA distinguishes six levels that determine the impact of personal data breaches on individuals. The higher the number, the higher the impact on the individual. An overview of the various kinds (nature) of data breaches and types of exposure is presented in Figure 8. Based on this figure, ENISA concludes that the severity of a personal data breach that only contains unauthorized or unlawful access (read access only) can be classified as very low/negligible (a rating of "1" in Figure 8) and disclosure of personal data as very high (a rating of "4" in Figure 8). This is difficult to understand, because even unauthorized or unlawful access (that for instance includes copying personal data) can have severe consequences for the rights and freedoms of individual data subjects. For this reason the category of 'unauthorized or unlawful access' will not be included in the de minimis rule (although according to ENISA the adverse impact is very low/negligible).

Nature of data breach / type of exposure	
Type	**Exposure**
Unauthorised or unlawful access (read access only)	1
Loss or destruction	2
Minor alteration / modification of personal data	3
Transmission	3
Major alteration / modification of personal data	4
Disclosure (e.g. to public or unauthorized third parties)	4

Figure 8: Parameters to determine the impact of the nature of data breach/ type of exposure of personal data breaches to the individual (ENISA, 2012; 55-56). Very Low/Negligible, Medium, High, Very High, corresponding to values of 1, 2, 3, 4.

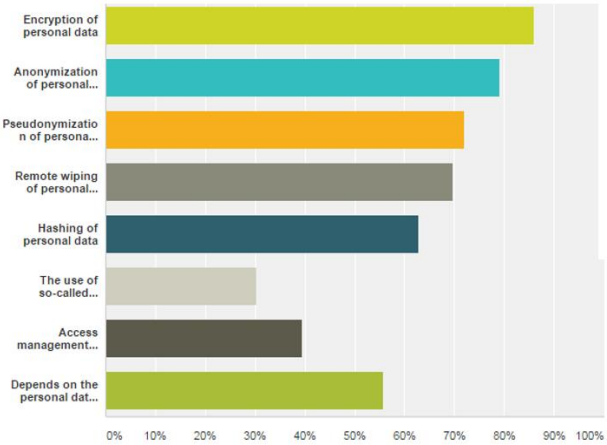
5.2.6. Data chain effect

24 (52.17%) of the 46 respondents have stated that the criterion of a stand-alone personal data set in combination with other personal data sets can be applied to formulate a de minimis rule for personal data breach notifications. However 24 (82.76%) of the 29 respondents stated that the specific categorization depends on the personal data breach and its specific context. The data chain effect

resembles the cybernation dimension that has been formulated by Etzioni (2015b) as part of his Cyber Age Privacy Doctrine (CAPD). Also the Dutch Data Protection Authority refers to the notion of cybernation, both in its background study of personal data and risk-classification (2001) - in which a distinction is made between 'low complexity of processing' and 'high complexity of processing' – and in its policy rules regarding the data breach notification obligation as included in the Dutch Data Protection Act (Dutch Data Protection Authority, 2015; 28). The use of multiple personal data sources, as for instance applied in the context of profiling, is of a qualitative nature and cannot be applied to a de minimis rule. The use of multiple personal data sources by sharing, collating and combing personal data, probably will generate more risks to the rights and freedoms of data subjects compared to single sources of personal data. However it would be too easy to conclude that personal data breaches that affect only one source of personal data, can be exempted from the personal data breach notification, as this single source for instance can also contain sensitive personal data that can impose severe privacy risks upon the data subject. The criterion of the data chain effect can only be applied in combination with the other criteria to assess whether notification of the personal data breach to the supervisory authority (and communication to the individual data subject who is affected) is necessary. It cannot be used as stand alone criterion to formulate a de minimis rule.

5.2.7. Mitigation measures

43 (95.56%) of the 45 respondents stated that mitigation measures can be applied to formulate a de minimis rule for personal data breach notifications. Figure 9 shows the different types of mitigation measures that can be applied, as indicated by the respondents.



Answer Choices	Responses	
Encryption of personal data	86.05%	37
Anonymization of personal data	79.07%	34
Pseudonymization of personal data	72.09%	31
Remote wiping of personal data	69.77%	30
Hashing of personal data	62.79%	27
The use of so-called internal "Chinese Walls"	30.23%	13
Access management strategies	39.53%	17
Depends on the personal data breach and its specific context	55.81%	24

Figure 9: Overview of mitigation measures (and scores of respondents) that can be applied as part of a de minimis rule for personal data breach notifications (43 respondents)

These findings support the conclusions of ENISA (2011), the Dutch Data Protection Act and the Dutch Data Protection Authority (2015). The policy rules of the Dutch Data Protection Authority state that if a controller has taken adequate protection measures to render the relevant personal data incomprehensible or inaccessible as consequence of a personal data breach, there is no need to notify the supervisory authority and inform the data subject *if a back-up of the personal data is available*. This means that adequate security measures such as encryption, hashing and remote

wiping can be applied to prevent notification of personal data breaches to the supervisory authorities and communication to data subjects who are affected (in cases when a back-up is available).

5.3. Construction of a de minimis rule

Based on the criteria that have been discussed in this chapter, a de minimis rule for personal data breach notification can be formulated. First and foremost it is important to stress that not one single and individual criterion can be applied on an individual (i.e. stand-alone) basis to formulate a de minimis rule for personal data breach notifications. A de minimis rule can only be formulated as a combination of various criteria. The Irish case in which notification of personal data breaches to the Irish Data Protection Commissioner is not necessary when three conditions are met (i.e. less than 100 persons affected, the breach only includes non-sensitive personal data and the breach is a promptly notified to the data subjects who are affected) is a good example of the combined application of various criteria. Also the notion of high risk data processing activities as included in the GDPR, is built upon the point of view that the *combination* of various individual criteria define a high risk category (e.g. new technology combined with large scale processing of personal data).

A de minimis rule would then be based upon *all* of the following conditions (i.e. non-exclusive). There is no need to notify personal data breaches to the supervisory authority (and to communicate it to the individual data subject who is affected) if only public personal data is involved (i.e. risk class 0 as defined by Blarkom and Borking, 2001), it only concerns one individual data source and if the financial damage to the individual data subject is limited to € 500. When personal data is stored on individual devices and data carriers such as laptops, mobile phones, USB sticks and CD ROMs that are stolen or compromised, notification to the supervisory authority (and communication to the individual data subject who is affected) is not necessary when the controller has taken adequate security measures to render the relevant personal data incomprehensible or inaccessible and a back up of the affected personal data is available.

A de minimis rule for personal data breach notifications therefore does not include a threshold for the number of personal data items or the number of data subjects that are affected, nor does it include a time threshold for notification. Notification for example is deemed necessary if it concerns sensitive data from one individual data subject, but it may *not* be necessary to notify in case a large group of data subjects are affected if it concerns ´only´ public data from one single source with a individual financial damage of less than € 500. Earlier on in this chapter the time period for which the personal data was collected or retained, was considered not to be relevant for the construction of a de minimis rule, because a minority of the respondents (40.43%) classified this criterion as non-relevant for the construction of a de minimis rule. ENISA (2012; 57) however has identified the delay in identifying the breach as relevant parameter to measure the level of exposure of a personal data breach. Although time can be a relevant parameter to measure the impact of a personal data, it is not relevant for the construction of a de minimis rule. The time after which the personal data will be notified (and the delay that might occur in the notification) is relevant to assess the risk to the rights and freedoms of the data subject, but prompt notification will not cause the risk to be negligible or absent. Breaches that are

notified promptly to the supervisory authority still can have serious effects on the rights and freedoms of the data subject, for instance in case of loss of sensitive personal data. The same can be said about the duration of the personal data breach. A long duration of a personal data breach (e.g. in case the personal data breach has been discovered after some weeks or months) will have impact on the risks to the rights and freedoms of data subjects. Nonetheless also personal data breaches (for instance a hack to a ICT system) with a short duration can have a serious impact because the personal data can be copied and transferred in seconds, after which the personal data will be in the public domain and the damage has been done.

A word can be said about the geographical scope of personal data that will be processed as relevant criterion for the construction of a de minimis rule for personal data breach notifications. Although this criterion is included in the NIS Directive (2016) for the notification of incidents that have a significant impact on the continuity of essential services or have a substantial impact on the provision of digital services, it will not be taken into account for the construction of a de minimis rule. First this criterion is applied in the NIS Directive to measure the impact of incidents on the *continuity and provision* of services, and not to measure the impact of those incidents on the rights and freedoms (i.e. the respect for private and family life and the protection of personal data) of data subjects. It seems relevant to include the geographical scope of an incident to measure the impact of an incident on the discontinuity of services, but less or non-relevant to take this criterion into account to measure the impact of an incident that involves the loss or alteration of personal data for *individual* data subjects. Also the question whether a personal data breach has an occasional or structural character is not relevant to determine a de minimis rule for personal data breach notifications. As was indicated in chapter 2 of this thesis, unintentional personal data breaches represent the largest category of personal data breaches (Symantec, 2016; 51)(Verizon, 2015; 31). The severity and likelihood of personal data breaches on the rights and freedoms of data subjects therefore are not dependent on the answer to the question of such a breach was caused by an (human) error or caused on purpose. Both occasional and structural personal data breaches can have a severe impact and a high likelihood. It therefore does not make sense to apply this criterion as building block for the formulation of a de minims rule.

5.4. Conclusion

Most respondents (52 (96,11%) of the respondents of the online questionnaire indicated that the type of personal data (sensitive/ non-sensitive) that will be processed, is the most important criterion for any privacy risk assessment. A majority of the respondents of the online questionnaire refer to the type of personal data *(*(44) 93.62% of respondents), the material and non-material damage to natural persons that is caused by the privacy infringement ((30) 65.22%%), ((30) 65.22%), the nature of personal data breaches ((27) (60%)), the purpose of processing of personal data ((29) 56.86%), the number of personal data items that will be processed ((28) 54.90%), the number of persons of which personal data will be processed ((27) 50.98%) and the processing of a stand-alone personal data set in combination with other personal data sets (data chain effect) ((24) 52.17%) as criteria that can be used to formulate a de minimis rule for personal data breach notifications.

Based on the criteria that have been discussed in this chapter, a de minimis rule for personal data breach notification can be formulated. First and foremost it is important to stress that not one single and individual criterion can be applied on an individual (i.e. stand-alone) basis to formulate a de minimis rule for personal data breach notifications. A de minimis rule can only be formulated as a combination of various criteria. The Irish case in which notification of personal data breaches to the Irish Data Protection Commissioner is not necessary when three conditions are met (i.e. less than 100 persons affected, the breach only includes non-sensitive personal data and the breach is a promptly notified to the data subjects who are affected) is a good example of the combined application of various criteria.

A de minimis rule would then be based upon *all* of the following conditions (i.e. non-exclusive). There is no need to notify personal data breaches to the supervisory authority (and to communicate it to the individual data subject who is affected) if only public personal data is involved (i.e. risk class 0 as defined by Blarkom and Borking, 2001), it only concerns one individual data source and if the financial damage to the individual data subject is limited to € 500. When personal data is stored on individual devices and data carriers such as laptops, mobile phones, USB sticks and CD ROMs that are stolen or compromised, notification to the supervisory authority (and communication to the data subject who is affected) is not necessary when the controller has taken adequate security measures to render the relevant personal data incomprehensible or inaccessible and a back up of the affected personal data is available.

Chapter 6: Conclusion

The central research question of this thesis is how a de minimis rule can be formulated for the notification and communication of personal data breaches in the GDPR as part of a privacy risk classification framework. A personal data breach can be defined as (quote): *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'* (GDPR, article 4, paragraph 12). A de minimis rule requires the formulation of a quantitative or qualitative threshold below which notification of a personal data breach to the supervisory authority and communication to the data subject is not mandatory, because the risk to the rights and freedoms of data subjects will be negligible.

Over the recent years, attention from governments worldwide has increased for personal data breach notification as regulatory instrument to force organizations to inform customers (and other stakeholders) about operational failures and enable customers to take appropriate measures to mitigate negative consequences of such breaches. Many personal data breach notification laws have been implemented worldwide over the last years (Nymity, 2016a, 2016b, 2016c). Government scrutiny also has been driven by the increased frequency and costs that are related to personal data breaches (Symantec, 2010)(Verizon 2015, 2016)(The Identity Theft Center, 2015, 2016)(Ponemon Institute, 2015, 2016). The increased attention for personal data breach notification obligations has also been reflected in European legislation. The revised e-Privacy Directive that was published at the end of 2009 (Directive 2009/136/EC, 2009) includes the obligation for the provider of publicly available electronic communications services to notify *all* personal data breaches to the competent national authorities. Contrary to the revised e-Privacy Directive, the personal data breach notification obligation of the GDPR is based on a risk-based approach. The reason to introduce the risk-based approach was the ambition to reduce the administrative burden/compliance costs for companies and to limit the number of notifications of personal data breaches that will be sent to the data protection authorities (Italian Presidency, 2014)(Council of the European Union, 2014a).

Article 33 of the GDPR states that the controller shall notify the personal data breach to the supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Article 34 of the GDPR states that when personal data breaches are likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject. The notions of risk and high risks have not been defined in the GDPR, nor does the GDPR contain a privacy risk classification framework. However, it can be concluded from the recitals and article 35 of the GDPR that high risk data processing activities will comprise profiling activities, large scale use of new technology, large scale processing of sensitive personal data and large scale (systematic) monitoring of publicly accessible areas. The GDPR also seems to suggest that low risks or no risks relating to data processing can exist, as for instance article 30 of the GDPR lifts an enterprise or organization with fewer than 250 employees from an obligation to maintain records regarding data processing, (quote*): 'unless the processing it carries out is likely to result in a risk for the rights and freedoms, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or*

personal data relating to criminal convictions and offences referred to in Article 10' (Article 30, paragraph 5, GDPR) (See also Schwarz, 2016). Moreover, article 35, paragraph 5 GDPR states that the supervisory authority may establish and make public a list of the kind of processing operations for which no data protection impact assessment is required, thereby implying that processing operations exist which do impose no or low risks to the rights and freedoms of data subjects. However examples of data processing that should be considered as low risks or no risks are not explicit incorporated in the text of the GDPR.

A technical risk assessment that is based on risk being defined (and calculated) by the probability and the harm that is caused by a threat, seems to fit the risk-based approach that is included in the GDPR. Building blocks for the construction of a privacy risk classification framework for personal data breach notifications in the GDPR can be found in publications of ENISA (2011)(2012), Etzioni (2015b), the German (2009), Canadian (2014), Austrian (2010) and the Dutch Data Protection Act (2015), the Irish Personal Data Security Breach Code of Practice (2011), background study and guidelines of the Dutch Data Protection Authority (2001)(2015), publications of the Centre of Information Policy Leadership (2014a, 2014b, 2014c, 2016a, 2016b) and the NIS-Directive (2016). All these sources have in common that they center around three categories of qualitative criteria that determine the risk to the rights and freedoms of data subjects relating to personal data breaches, i.e. criteria that relate first to the *nature of the affected data* (such as sensitive or no-sensitive personal data), second to the *nature and extent of the affected processing* (such as number of data subjects affected, cybernation, geographical spread, profiling, (non) structural character of breach and duration of breach) and third to adequate *security measures* to protect the personal data and mitigate the impact of personal data breaches (such as encryption or remote wiping).

A de minimis rule for personal data breach notifications can be formulated as a combination of various criteria and would be based upon *all* of the following conditions (i.e. non-exclusive). There is no need to notify personal data breaches to the supervisory authority (and to communicate it to the individual data subject who is affected) if only public personal data is involved (i.e. risk class 0 as defined by Blarkom and Borking, 2001), it only concerns one individual data source and if the financial damage to the individual data subject is limited to € 500. The amount of € 500 is based on the application of the de minimis rule that is included in article 35, paragraph 3, under b) of the European Convention on Human Rights (ECHR). When personal data is stored on individual devices and data carriers such as laptops, mobile phones, USB sticks and CD ROMs that are stolen or compromised, notification to the supervisory authority (and communication to the individual data subject who is affected) is not necessary when the controller has taken adequate security measures to render the relevant personal data incomprehensible or inaccessible and a back up of the affected personal data is available. A de minimis rule for personal data breach notifications therefore does not include a threshold for the number of personal data items or the number of data subjects that are affected, nor does it include a time threshold for notification. Also the geographic scope of the personal data breach and the answer to the question whether the personal data breach did have an occasional or structural character, is not relevant for the construction of a de minimis rule.

A final word has to be said about the question whether the building blocks for the construction of a privacy risk classification framework and the formulation of a de minimis rule as presented in this thesis, will be relevant for the evaluation of the revised e-Privacy Directive (Directive 2009/136/EC, 2009). The current revised e-Privacy Directive includes a personal data breach notification for providers of publicly available electronic communications services providers, but does not contain a risk threshold for the notification of personal data breaches to supervisory authorities and the communication to the data subjects who are affected. At this moment the revised e-Privacy Directive is being evaluated by the European Commission, so the inclusion of such a risk threshold seems to be a timely opportunity. However, it will be likely that the personal data breach notification obligation that is included in the revised e-Privacy Directive will be eliminated to avoid duplications vis-à-vis the notification obligation that is already incorporated in the GDPR. That is at least the advice given by the Article 29 Data Protection Working Party (2016a; 19) and the European Data Protection Supervisor (2016; 19).

Literature list

Ablon, Lillian, Heaton, Paul, Lavery, Diana Catherina and Sasha Romanosky (2016), "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information", RAND Corporation

Acquesti, Allesandro, Friedman, Allan and Rahul Telang (2006), "Is There a Costs to Privacy Braches? An Event Study". In: Proceedings of the Twenty-Seventh International Conference on Information Systems.

Adler, Matthew D. (2007), "Why De Minimis?", Institute for Law & Economics University of Pennsylvania Law School Research Paper No. 07-12, Public Law and Legal Theory University of Pennsylvania Law School Research Paper No. 07-26, University of Pennsylvania Law School, June 2007

Anderson, Ross, Barton, Chris, Bohme, Rainer, Clayton, Richard, van Eeten, Michel J.G., Levi, Michael, Moore, Tyler and Stefan Savage (2012), "Measuring the Cost of Cybercrime", 11th Annual Workshop on the Economics of Information Security

Article 29 Data Protection Working Party (2012), "Opinion on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications", Adopted on 12 July 2012, WP 197

Article 29 Data Protection Working Party (2016a), "Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)", Adopted on 19 July 2016, 16/ EN, WP 240

Article 29 Data Protection Working Party (2011), "Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications", Adopted on 11 February 2011, 00327/11/EN WP 180

Article 29 Data Protection Working Party (2016b), "Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)", Adopted on 2 February 2016, 442/16/EN WP 236

Article 29 Data Protection Working Party (2014a), "Statement on the role of a risk-based approach in data protection legal frameworks", Adopted on 30 May 2014, 14/EN WP 218

Article 29 Data Protection Working Party (2014b), "Opinion 03/2014 on Personal Data Breach Notification", Adopted on 25 March 2014, 693/14/EN, WP 213

Article 29 Data Protection Working Party (2013), "Statement of the Working Party on current discussions regarding the data protection reform package", 27.02.2013

Autoriteit Consument & Markt (2013), "ACM Jaarverslag 2013"

Autoriteit Consument & Markt (2014), “ACM Jaarverslag 2014”

Autoriteit Consument & Markt (2015), “ACM Jaarverslag 2015”

Baas, J.A.N. en M.H.J. van Rest (2012), “Informatie- en meldplicht bij datalekken en beveiligingsinbreuken”. In: Privacy & Informatie, Aflevering 6, december 2012, bladzijde 260-268.

Barabas, Emily (2015), “Privacy and Data Protection “Tour du Monde”, 37th International Conference of Data Protection and Privacy Commissioners, Commissioned by College Bescherming Persoonsgegevens, Researched and Written by Emily Barabas, October 2015

Beck, Ulrich (1986), “Risk Society, Towards a New Modernity”, Sage

Beck, Ulrich (1999), “World Risk Society”, Polity Press

Beck, Ulrich (2006), “Living in the world risk society”, A Hobhouse Memorial Public Lecture given on Wednesday 15 February 2006 at the London School of Economics. In: Economy and Society, Volume 35, Number 3, August 2006, page 329-345

Berg, Bibi van den (2016), “Regulating security in cyber space”, slides Professional MSc Program Cyber Security, Cyber Security Academy, day 4, block 1, 08 January 2016

Bijlsma, Michiel, Straathof, Bas and Gijsbert Zwart (2014), “Choosing privacy, How to improve the market for personal data”, CPB Policy Brief, 2014/4

Blakley, Bob, McDermott, Ellen and Dan Geer (2001), “Information Security is Information Risk Management" In: NSPW '01 Proceedings of the 2001 workshop on New security paradigms, Pages 97-104

Blarkom, G.W. van en drs. J.J. Borking (2001), "Beveiliging van persoonsgegevens", Achtergrondstudies en Verkenningen 23, Registratiekamer, Den Haag, april 2001

Boutellier, Hans et al (2005), "Leven in een risicosamenleving", Salomé

British Standard ISO/IEC 27005 (2008), “Information technology – Security techniques – Information security risk management”, BSI British Standards

Brooks, Sean and Ellen Nadeau (2015), “Privacy Risk Management for Federal Information Systems”, NISTIR 8062 (Draft), National Institute of Standards and Technology (NIST), May 2015

California S.B. 1386 (2003), California Security Breach Information Act

Centre for Information Policy Leadership (2014a), Hunton & Williams LLP, “A Risk-based Approach to Privacy?" An Initial Issues Paper for Privacy Risk Framework and Risk-based Approach to Privacy Project, Workshop I, Paris, France, 20 March 2014

Centre for Information Policy Leadership (2014b), Hunton & Williams LLP, “A Risk-based Approach to Privacy? Improving Effectiveness in Practise", 19 June 2014

Centre for Information Policy Leadership (2014c), Hunton & Williams LLP, “The Role of Risk Management in Data Protection, Paper 2 of the Project on Privacy Risk Framework and Risk-based Approach to Privacy”, 23 November 2014

Centre for Information Policy Leadership (2016a), Hunton & Williams LLP, “Protecting Privacy in a World of Big Data Paper 2 The Role of Risk Management”, DISCUSSION DRAFT 16 February 2016

Centre for Information Policy Leadership (2016b), Hunton & Williams LLP, “”Risk", "High Risk", Risk Assessments and Data Protection Impact Assessments under the GDPR, DRAFT 29 August 2016

Charter of Fundamental Rights of the European Union (2000/C 364/01), Official Journal of the European Communities, 18.12.2000

Chicken, John C. and Tamar Posner (1998), "The Philosophy of Risk", Thomas Telford

College bescherming persoonsgegevens (2015), “De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)”, Consultatieversie, 21 september 2015

Commission Nationale de l’Informatique et des Libertés (2012), “Methodology for Privacy Risk Management, How to Implement the Data Protection Act” (Translation of June 2012 edition)

Commission Nationale de l’Informatique et des Libertés (2015), “Privacy Impact Assessment (PIA), Methodology (how to carry out a PIA)”, June 2015 Edition

Commission Staff Working Document, Impact Assessment, Accompanying the document, Proposal for a Directive of the European Parliament and of the Council, Concerning measures to ensure a high level of network and information security across the Union, {COM(2013) 48 final} {SWD(2013) 31 final}, Strasbourg, 7.2.2013, SWD(2013) 32 final

Consolidated version of the Treaty on the Functioning of the European Union (TFEU) (2012), Official Journal of the European Union, C 326/47, 26.10.2012

Council of Europe (2004), "Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention", Council of Europe Treaty Series - No. 194, Strasbourg, 13.V.2004

Council of the European Union (2016), “Position of the Council at the first reading with a view to the adoption of a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures for a high common level of security of network and information systems across the Union”, Brussels, 21 April 2016, 5581/16

Council of the European Union (2014a), “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Risk based approach”, General Secretariat of the Council, Brussels, 2 September 2014, 12267/2/14

Council of the European Union (2014b), “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) **[First reading]** – Chapter IV”, Presidency, Brussels, 3 October 2014, 13772/14

Dentons (2016), "Data security and breach notification in Canada", September 25, 2016. Website (visited 23 October 2016): http://www.lexology.com/library/detail.aspx?g=a7378410-72cb-4d48-9f3f-4e4d1e748d7e

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the European Union, L 337, 18 December 2009.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (“NIS Directive”), Official Journal of the European Union, L 194/I, 19.7.2016

Dutch Data Protection Authority (2015), “The data breach notification obligation as laid down in the Dutch Data Protection Act, Policy rules for the application of article 34a under the Dutch Data Protection Act”, 8 December 2015

Ernst & Young (2015), “Creating trust in the digital world, EY’s Global Information Security Survey 2015”

Etzioni, Amitai (2013), “A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach”. In: A Journal of Law and Policy for the Information Society, Vol. 10, Issue 2 (Summer 2014), October 1, 2013

Etzioni, Amitai (2015a), “A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational”. In: Brooklyn Law Review , Vol. 80, No. 4, 2015

Etzioni, Amitai (2015b), “Privacy in a Cyber Age, Policy and Practice”, Palgrave MacMillan’s studies in Cyber Crime and Security, Palgrave Macmillan

Etzioni, Amitai (1998), “The New Golden Rule, Community and Morality in a Democratic Society”, the Perseus Books Group, March 1998

European Commission (2009), Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radiofrequency identification (2009/387/EC), Official Journal of the European Union L 122/47, 16.05.2009

European Commission (2000), "Communication from the Commission on the precautionary principle", Brussels, 2.2.2000, COM(2000) 1 final

European Commission (2013), “Commission Regulation (EU) no 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and the Council on privacy and electronic communications”, Official Journal of the European Union, L 172/2, 26.6.2013

European Commission (2012), “Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”, Brussels, 25.1.2012, COM(2012) 11 final 2012/0011 (COD)

European Commission (2014a), “Commission Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice)”, Official Journal of the European Union, C 291, 30 August 2014

European Commission (2014b), “Commission Staff Working Document, Guidance on restrictions of competition "by object" for the purpose of defining which agreements may benefit from the De Minimis Notice, Accompanying the document COMMUNICATION FROM THE COMMISSION Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice), REVISED VERSION OF 03/06/2015, Brussels, 25.6.2014 SWD(2014) 198 final, {C(2014) 4136 final}

European Commission (2001), "Commission Regulation (EC) No 69/2001 of 12 January 2001 on the application of Articles 87 and 88 of the EC Treaty to de minimis aid", Official Journal of the European Communities, 13.1.2001, L 10/30

European Court of Human Rights (2012), "Research Report, The new admissibility criterion under Article 35 § 3 (b) of the Convention: case-law principles two years on"

European Data Protection Supervisor (2016), “Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)”, 22 July 2016

European Network and Information Security Agency (ENISA) (2011), “Data breach notifications in the EU”

European Network and Information Security Agency (ENISA) (2012), “Recommendations on technical implementation guidelines of Article 4”

European Network and Information Security Agency (ENISA) (2016), Glossary published under risk management, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary (visited 15 September 2016).

Frick, David E. (2012), “The Fallacy of Quantifying Risk.” In: Defense AT&L, September-October 2012

Gellert, Raphaël (2015), “Understanding Data Protection as Risk Regulation”, Journal of Internet Law, May 2015

Hallinan, Diarmuid (2011), "Data Breach Code of Practice", Office of the Data Protection Commissioner Ireland, ENISA Workshop on Data Breach Notification, 24 January, 2011

Hogan Lovells (2014), Chronicle of Data Protection, “Prepare Yourself for the “Risk-Based” Approach to Privacy”, Posted on October 28th, 2014 By Eduardo Ustaran

Hojnik, Janja (2013), “De Minimis Rule within the EU Internal Market Freedoms: Towards a More Mature and Legitimate Market?” In: European Journal of Legal Studies, Volume 6, Issue 1 (Spring/Summer 2013), p. 25-45

Holvast, Jan (1986), "Op weg naar een risicoloze maatschappij? De vrijheid van de mens in de informatiesamenleving", Academic Service

Hunton & Williams (2014), “Council of the European Union Proposes Risk-Based Approach to Compliance Obligations”, Privacy & Information Security Law Blog, Posted on October 29, 2014

Hunton & Williams, Cognicion and FireEye (2016), “Hot Topics in Cybersecurity”, 3 November 2016 (recording and presentation)

Information and Privacy Commissioner Ontario (2010), "Privacy Risk Management, Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, *by default",* April 2010

Identity Theft Resource Center (2016), 2016 Data Breach Stats, Report Date: 4/26/2016.

Identity Theft Resource Center (2015), Data Breach Reports, December 31, 2015

Information Commissioner’s Office (ICO) (2014), ”Conducting privacy impact assessments code of practice”, February 2014

Information Commissioner's Office (ICO) (2009), "Privacy Impact Assessment Handbook", Wilmslow, Cheshire, UK, December 2007, Version 2.0, June 2009

Information Commissioner's Office (2016), "Data Protection Act 1998, Supervisory Powers of the Information Commissioner, Monetary Penalty Notice to TalkTalk Telecom Group PLC", 30 September 2016

International Organization for Standardization (ISO) (2005), "Information technology — Security techniques — Code of practice for information security management", ISO/IEC 27002, First edition, 15 June 2005

International Organization for Standardization (ISO) (2009), "Risk management – Principles and Guidelines", ISO 31000: 2009

ISO/IEC 27005 (Second edition) (2011), "Information technology – Security techniques – Information security risk management", Reference number ISO/IEC 270005:2011(E), 01.06.2011

Italian Presidency (2014), "Risk-based approach in EU General Data Protection Regulation, brief state of work in the EU Council (Italian Presidency)"

Lynskey, Orla (2015), "The Foundations of EU Data Protection Law", Oxford Studies in European Law

LIBE Committee (2013), "Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2013)", Inofficial consolidated version after LIBE Committee vote provided by the Rapporteur, 22 October 2013

Maldoff, Gabriel (2016), "The Risk-Based Approach in the GDPR: Interpretation and Implications", International Association of Privacy Professionals (IAPP)

Maurushat, A. (2009), "Data Breach Notification Law Across the World from California to Australia", University of New South Wales research paper 2009-11. In: Privacy Law and Business International 2009 (February)

Moerel, Lokke and Corien Prins (2016), "Privacy voor de homo digitalis, Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van big data en Internet of Things". In: Homo Digitalis, Preadviezen van E.M.L. Moerel en J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J Zwenne en A.H.J. Schmidt, Handelingen Nederlandse Juristen-Vereniging, 146e jaargang/2016-I, Wolters Kluwer

National Cyber Security Centre (2015), Ministry of Security and Justice, "Cyber Security Assessment Netherlands CSAN 2015", November 2015

National Institute of Standards and Technology (NIST) (2012), U.S. Department of Commerce, "Guide

for Conducting Risk Assessments", Joint Task Force Transformation Initiative, Information Security, NIST Special Publication 800-30 Revision 1, September 2012

National Institute of Standards and Technology (NIST) (2011), “Managing Information Security Risk Organization, Mission, and Information System”, Joint Taskforce Transformation Initiative, Information Security, NIST Special Publication 800-39, March 2011

NEN-ISO 31000 (en) (2009), "Risk management, Principles and guidelines" (ISO 31000: 2009, IDT)

New Zealand Government (2014), Internal Affairs, Te Tari Taiwhenua, “Risk Assessment Process, Information Security”, February 2014

Nymity Research (2016a), “Breach Response Table”, 2016

Nymity Research (2016b), “Europe Breach Response Table”, 2016a

Nymity Research (2016c), “Global Breach Response Laws”, 2016b

Office of the Privacy Commissioner (2010), “Privacy Impact Assessment Guide”, Sydney, 2006, revised 2010

Onafhankelijke Post en Telecommunicatie Autoriteit (2012), “Jaarverslag 2012”

Peterson, Martin (2002), “What is a de Minimis Risk?”, In: Risk Management 4, page 47–55, Perpetuity Press Ltd

Ponemon Institute (2015), “2015 Cost of Data Breach Study: Global Analysis”, Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute LLC, May 2015

Ponemon Institute (2016), “2016 Cost of Data Breach Study: Global Analysis”, Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute LLC, June 2016

PRESCIENT (2013), “Deliverable 4: Final Report – A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies”, Editors: Venier, Silvia and Emilio Mordini

Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011

Quelle, Claudia (2015), “The Data Protection Impact Assessment, What can it contribute to data protection?”, Thesis for the Research Master in Law and the Master’s program Law and Technology 2013-2015

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4 May 2016

Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity), Tweede Kamer, vergaderjaar 2015–2016, 34 388, nr. 2, Voorstel van wet

Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity), Tweede Kamer, vergaderjaar 2015–2016, 34 388, nr. 3, Memorie van Toelichting

Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity), Tweede Kamer, vergaderjaar 2015–2016, 34 388, nr. 6, Nota naar aanleiding van het verslag

Roeser, Sabine, Hillerbrand, Rafaela, Sandin, Per and Martin Peterson (2013), "Essentials of Risk Theory", Springer Briefs in Philosophy, Springer

Schwartz, Paul (2016), “Risk and high risk: Walking the GDPR tightrope”, Privacy Perspectives, 29 March 2016, https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/

Schwartz, Paul and Edward Janger (2007), “Notification of Data Security Breaches”

Staatssecretaris van Veiligheid en Justitie (2012), “Brief van de Staatssecretaris van Veiligheid en Justitie”, Verwerking en bescherming persoonsgegevens, 23 oktober 2012, Tweede Kamer, vergaderjaar 2012–2013, 32 761, nr. 44

Stoneburner, Gary, Alice Goguen and Alexis Feringa (2002), “Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology”, National Institute of Standards and Technology (NIST), Special Publications 800-30

Symantec (2016), “2016 Internet Security Threat Report”, Volume 21, April 2016

Taleb, Nassim N., Daniel G. Goldstein and Mark W. Spitznagel (2009). “The Six Mistakes Executives Make in Risk Management.” In: Harvard Business Review (October 2009), Harvard Business School Publishing Corporation.

Taleb, Nassim Nicolas (2012). “De Zwarte Zwaan. De impact van het hoogst onwaarschijnlijke”, Tweede editie, inclusief postscript essay ‘Over robuustheid’”. Uitgeverij Nieuwezijds.

Tana, Laura Vivet (2013), “EU Data Breach Notification Rule: The Key Elements”, The Privacy Advisor, August 27, 2013.

Tancock, David, Pearson, Siani, Charlesworth, Andrew (2010), "Analysis of Privacy Impact Assessments within Major Jurisdictions", 2010 Eight Annual International Conference on Privacy, Security and Trust.

Trilateral Research & Consulting (2013), “Privacy impact assessment and risk management Report for the Information Commissioner’s Office prepared by Trilateral Research & Consulting”, 4 May 2013

Thierer, Adam D. (2014), "Privacy Law’s Precautionary Principle Problem", Maine Law Review 66 (2): 467–86

TU Delft (2016), “Risk Management Summer Course”, Mon 4th – Fri 15th July 2016, Delft, The Netherlands

Tweede Kamer (2015), Meldplicht datalekken, Handelingen, TK 51, 5 februari 2015

Ustaran, Eduardo (2012), “European Privacy, Law and Practice for Data Protection Professionals”, An IAPP publication

Ustaran, Eduardo (2014), “Prepare Yourself for the ‘Risk-Based’ Approach to Privacy”, Hogan Lovells, Chronicle of Data Protection, Privacy & Information Security News & Trends, Posted on October 28th By Eduardo Ustaran

Verizon (2015), “2015 Data Breach Investigations Report”

Verizon (2016), “2016 Data Breach Investigations Report”

Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp) (amendment of the Dutch Data Protection Act).

Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik meldplicht datalekken), nr. 3 Memorie van Toelichting, Tweede Kamer, vergaderjaar 2012–2013, 33 662, nr. 3 (2013), 25 juni 2013

Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik meldplicht datalekken), nr.6 Nota naar aanleiding van het Verslag, Tweede Kamer, vergaderjaar 2012–2013, 33 662, nr. 6 (2014a), 16 april 2014

Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de

invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik meldplicht datalekken), nr.7 Nota van Wijziging, Tweede Kamer, vergaderjaar 2012–2013, 33 662, nr. 7 (2014b), 16 april 2014

Wijzigingswet Telecommunicatiewet (implementatie herziene telecommunicatierichtlijnen)(2012), Wet van 10 mei 2012 tot wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen

Wright, David and Paul de Hert (2012), “Privacy Impact Assessment”, Law, Governance and Technology Series 6, Springer

Zuiderveen Borgesius, F.J. (2011), “De meldplicht voor datalekken in de Telecommunicatiewet”. In: Computerrecht, Aflevering 2011, bladzijde 209-218