FROM RAISING BARRIERS TO RAISING ALARMS:

University of Oslo
Faculty of Law

Candidate number: 8001
Supervisor: Dr. Tobias Mahler
Deadline for submission: [12/01/2011]
Number of words: 15,223 (18,000)
01.12.2011
ABSTRACT

The Directive 2009/136/EC required the implementation of a Personal data breach notifications regime. This notification is a complement to the already existing Information Security Provisions. Information Security traditional function is to prevent the unauthorized access or disclosure of personal data. As modern technology was adopted into the processing of personal data, the risks inherent to such technology threaten the personal data being processed. The responsibility was placed over the controllers and processors, but as data breaches were more commonly related to Identity theft cases, other measures were necessary to prevent the controller to remain silent if affected by a breach.

California was the first jurisdiction to implement a mandatory regime of personal data breach notifications. In Europe, Spain and Germany implemented such notifications before the reforms to the E-Privacy Directive where adopted. As this date Personal Data Breach Notification Provisions are mandatory throughout the territory of the EU.

These notifications have as main function to give notice to the data subjects about the occurrence of a data breach that affects or its believed have affected, their personal data. The providers of publicly available electronic communication services in the Telecommunication sector are the only controllers who are obligated to perform the notification to both the National Data Protection Authorities or to the data subjects.

The present thesis reviews these provisions and analyses them in the context of the information security measures provisions. Discusses the threshold for appropriateness and develop on the traditional function that the information security had: to prevent unlawful access to or disclosure of personal information.

Since the model of the notification provision resembles the one applied in California, reference to this framework will be made. Also the national provisions in Germany, Ireland, the United Kingdom and Spain will be taken as reference to compare the different approach that member states have taken to comply with the implementation of the reforms that unsaturated the notification regime. Finally, notes to consider for future reforms will be presented.
List of Abbreviations

DPD  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


EU  European Union

29WP  Directive 95/46 EC Article 29 Working Party

NDPA  National Data Protection Authority

ENISA  European Network and Information Security Agency

EDPS  European Data Protection Supervisor


SDPL  Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, España.

BDSG  Federal Data Protection Act (BDSG) In the version promulgated on 14 January 2003 (Federal Law Gazette I, 66), last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, 2814), in force from 1 September 2009, Germany
Content
1 Introduction ....................................................................................................................7
2 Data Protection and Information Security .................................................................12
   2.1 Overview .................................................................................................................. 12
   2.2 Data Protection principles and their synergy ............................................................ 12
       2.2.1 Effects of the synergy of the information security principle with other data    protection principles ..................................................................................................... 13
   2.3 Information Security Goals .................................................................................... 17
   2.4 Risks ......................................................................................................................... 19
   2.5 Rights and obligation of Data Protection Actors, regarding Information Security.... 20
   2.6 Conclusion ............................................................................................................... 23
3 Preventive Security Measures .......................................................................................24
   3.1 Overview .................................................................................................................. 24
   3.2 About the appropriate level of security .................................................................... 24
       3.2.1 Access and Use limitation .................................................................................. 27
       3.2.2 Secure transmission, secure storage ................................................................. 29
       3.2.3 Security policy .................................................................................................. 30
       3.2.4 Encryption ......................................................................................................... 31
       3.2.5 Security risks warning ...................................................................................... 32
   3.3 Information Security Provisions in Germany and Spain .......................................... 32
   3.4 Conclusion ............................................................................................................... 36
4 Data breach and Notifications ......................................................................................38
   4.1 Overview .................................................................................................................. 38
   4.2 Introduction ............................................................................................................... 38
       4.2.1 What is a personal data breach? ................................................................. 39
       4.2.2 Who should be notified? ............................................................ 41
       4.2.3 When should a personal data breach be notified? ............................................ 42
       4.2.4 Form and content of a data breach notification ................................................ 46
       4.2.5 Other obligations arise after a data breach ....................................................... 47
   4.3 Conclusions ............................................................................................................. 49
5 Conclusion and criticism ..............................................................................................50
6 Bibliography ..................................................................................................................53
   6.1 Books ......................................................................................................................... 53
   6.2 Articles ...................................................................................................................... 53
1 Introduction

You are coming back to your house while birds sing to the last rays of light. The postman is driving out the same instant as you arrive. You search for the post and between the flyers and the postcard from your friend an envelope with the logo of your ISP immediately attracts your attention. You are sure (or at least you hope) it is not a new bill since you recently paid the monthly fee for the service. However, the content of the letter is different. A data breach has occurred. Personal data has been compromised. Yours and other customer’s personal data is in the possession of an unknown person with unknown intentions.

It may be that after reading the notification we find ourselves thinking how is it possible that in our world full of technology an organization can send a notification but have not done more to prevent this information security breach could to occur in the first place? What more could your ISP have done? They send a warning. This “alarm” has not always been there. At the start, the idea was prevention, not mitigation.

You might be angry knowing that someone has access to your political beliefs, sexual preferences or medical history. You might be scared as you realise the danger that is represented by a stranger knowing your bank account details or credit history. Should data controllers do better to secure our personal information? How can they increase their security?

Information is defined as ‘knowledge or facts that have been acquired (the information in the report). Data, news, background, revelation, intelligence, account, notes, wisdom, statistics, figures, enlightenment, understanding, communications, story, message…’\(^1\)

Black’s Law Dictionary, defines security as ‘freedom from harm.’ This definition refers to an ideal state in which no danger can affect nor exist, an ideal state that is constantly pursued. And though we never seem to fully reach it, we never stop trying. The Merrian–Webster dictionary, define it as ‘measures taken to guard against espionage or sabotage, crime, attack, or escape.’\(^2\) This second definition refers to the mediums employed to ensure security. Security is the goal.


Security measures recognise the risk that a data subject may be subjected to when their data is collected and stored by others. The collection of such data and the risks which may incur are acknowledged in the Directive 95/46/EC ("DPD") and Directive 2002/58/EC ("EPD").

The DPD was adopted by the European Parliament in 1995. The directive took the post of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data that had been adopted in 1981. The convention included a rule for security measures in its Article 7: 'Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.'

The Directive paraphrased the content of the Article 7 of the convention and went a step further by introducing considerations to be accounted for before implementing the security measures. Article 17 of the DPD mentions that the state of the art and costs of implementation had to be contrasted with the risk represented by the process and the nature of the information processed.

The obligation to implement security measures ensures that a data controller will make his best effort to achieve a certain level of security. Such measures require that the protection given to personal data should be appropriate enough to grant a level of confidence to National Data Protection Authorities ("NDPA") and data subjects. In accomplishing this goal, the controllers and processor carry the obligation while data subjects have no such obligations.

Given the onset of new technology and growth of services on the internet, the European Parliament grew concerns for the situation presented for personal data transmission in the telecommunication sector as ‘publicly available electronic communications services over the Internet open new possibilities for user but also new risks for their personal data and privacy’. Identity theft was becoming more usual although there were still not many cases. In 2002, the new EPD replaced the Directive 97/66/EC and became the new translation of ‘the principles set out in Directive 95/46/EC into specific rules for the Telecommunication sector’.

---

3 DPD Recital 53
EPD Recitals 20 and 21.
4 EPD Recitals 7.
5 Ibid Recital 4
In most of the world, information security measures had as goal to offer security by preventing leaks of information and to suppress intrusions and attacks that could lead to unauthorized disclosure of personal data. In other parts of the globe, the legislators were ready to take security provisions a step further.

While identity theft cases start growing in Europe, data subjects in the U.S. have already experienced this threat for several years. In 2003, the State of California adopted the Database Security Breach Notification Act in an attempt to minimize the effects of data breaches. Their model was adopted by other states later, without modification in some cases. The main idea of giving warning to the data subject remained. The EU did not adopt the American approach immediately. Some member states like Germany and Spain went ahead and introduced data breach notification schemes, making it of mandatory observance for controllers and processors of personal data. The UK on the other hand stood on the position that such kind of law was not required.

In 2009, the Directive 2009/136/EC ("CKD") amended the EPD and instituted the data breach notification scheme though it limited to providers of public available electronic communication services in the European Union. The data breach notification provisions were not mandatory at the European level until May 2011, when the implementation at the national level had to be concluded.

On 4 May 2011, the UK transposed the EPD word-by-word, and the changes took effect 26 May of this year. By the date, the Information Commissioners’ Office had emitted guidelines for cases when data breach occurs. Ireland extended the reach of the data breach notification scheme as implemented in the EPD. The Statutory Instrument 336 represents the formal

---

6 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, España.


9 Guidance on data security breach management V2.0 July 2011 Information Commissioner’s Office UK.
implementation of the Directive performed by the Data Protection Commissioner and is limited for Publicly Available Electronic Communications Service Providers (ECSP). As well as this, the Data Protection Commissioner issued a Code of Practice for controllers and processor of personal data in other sectors than the Telecom which was ruled by the implementation of the EPD.

The introduction of such obligation for ECSP complemented the spectrum of security measures. By adding a notification schemes as part of the security measures, the reach of the "secure process principle" of data protection has extended to include controllers, processors and the data subject. From being an extra, data subjects were brought to the spotlight and given a small role. These reforms also benefit the industry as the data subjects were moved forward to have a more active role in protecting their own privacy. Security was no longer only about "prevention" as notifications in case of data breach are aimed to suffocate and minimize eventual damages in cases of information security violations.

Controllers and processors of data have the obligation to implement security measures for personal data processing, regardless of the sector in which they belong. But there is no express obligation for data controllers that requires them to notify data subjects if an information security breach occurs, as it is for the ECSPs.

The information security provisions in Article 4 of the EPD are more specific than those stated in the DPD. For the characteristic of the service they provide, ECSP’s functions are more related to the functions of a processor. The obligation to notify the data subjects was initially envisioned for controllers of personal data. ECSP also have the obligation to notify the data subjects, which implies a bigger responsibility than for data processors in other sectors.

---


12 California Civil Code § 1798,82 (a). The rule observe that the owner of licence of computerized data must notify the data subject. In the case that a person of business that maintains computerized personal data should only notify the owner of the licence.
The data breach notification stands as a warning for data subjects. It serves as a sign about the dangers that stem from having personal data compromised. This thesis will explore the role of data breach notifications, their threshold, and the role of data subjects when a breach has or could have occurred. The content of the notification obligation will be reviewed and explained to clarify the legal mechanism that surround the Personal Data Breach Notification scheme.
2 Data Protection and Information Security

2.1 Overview

This chapter aims to describe the data protection principles. In particular, it will focus on the information security principle and its synergy with other principles in order to assess such, against the information security measures under the current data protection regime implemented under the EPD.

The synergy of the Data Protection Principles will be looked at and the effects of such synergy as they define the security measures which must be met under the current regime. Afterwards, a short description of the causes for a personal data breach and the risk that such poses for the data subject will be provided in conjunction with a review of the roles of the data protection actors in regards to the information security which they are required to provide.

2.2 Data Protection principles and their synergy

“Fair and Lawful Processing” is the main principle of data protection law.¹³ This principle makes reference to the conditions under which the processing of personal data should be carried out in each of its phases, from the input to the output, collection, deletion and everything in between. In the EU legal context, the main manifestation of this principle is to be found in the Article 6(1)(a) of the DPD which provides that “fairly and lawfully” is how personal data must be processed. In general, all the provisions of data protection will have “legal” or “fair” character, being easier to determinate what is legal than what would stands as “fair”, for the social connotations that this concepts involves. Other principles are derived from this main principle, as branches are grown from the trunk of a tree, and as branches, some overlap other’s functions in determinate circumstances, as will be shown further in this chapter.

The “information security” principle manifests in the obligation to implement security measures to the processing of personal data. The data controller is obliged to install, maintain and support measures to ensure the integrity of the information and the integrity of the

---

process ‘to ensure that personal data are not destroyed accidentally and not subject to unauthorized access, alteration, destruction or disclosure’.  

Article 17 of the DPD provides 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’.

This obligation, as mentioned before, describes in general the terms of the goal of security information. The interaction between the data protection principles influences the application of the security measures. Security, in this sense, is not the only concern of security measures. Another important concern is the goal that other principles of data protection are achieved, as the needs of the security system have been redefined by the synergy between the data protection principles.

2.2.1 Effects of the synergy of the information security principle with other data protection principles

The data protection principles aim to guide certain stages, during the processing of personal data. The misapplication of one principle will have irremediably effects over the fairness and lawfulness of such process. Furthermore, some stages are affected by more than one principle which will have a knock-on effect on the interaction of such. This potential mismatch will in turn affect the synergy and dynamics of the principles and their actual affect, in reality, upon the processing personal data.

As mentioned above, Bygrave states that the Fair and Lawful processing is the core principle of data protection. It is difficult to think that all others are merely secondary, for all of them, including the Information Security Principle, are as important as the main principle. In practice, the lawfulness of the process will be assessed among other things for how security measures have been implemented. Because the DPD obliges data controllers to implement security measures to the process, it is implied that the lawfulness of the process will be determined by the level of security offered by the measures implemented to secure the process and the

14 Bygrave (n13) 67.
information collected, among other conditions. It can be concluded then, that the processing of personal data must have security measures implemented to be considered legal. However, the degree of such security is a key issue, for the Fair and Lawful processing of personal data requires that information security offering an appropriate level of security is implemented.

But do other principles of data protection have an effect on how security measures should also be implemented? Although each principle can be individualized, that does not necessarily mean that principles are fully independent, as it is undeniable that each principle has an effect on the others. Next, we will analyse how the synergy between the Information Security principle and other principles affect the way the first is applied in the implementation of information security measures.

2.2.1.1 The synergy of the Information security and Minimality principles

The “Minimality” principle is manifested in the Article 6(1)(c) of the DPD. It refers to the amount of information to be processed as they should be ‘not excessive in relation to the purposes for which they are collected and/or further processed.’

Another facet of this principle is manifested in the rule requiring ‘personal data to be erased or anonymised’ once it has served the purposes for which it was gathered and stored contained in Article 6(e) of the DPD. The less time data is used, the smaller the time frame will be for a data breach to occur.

In relation to the secure information principle, it can be observed that considerations regarding the amount of data and the duration of the process should be made while designing the process and during the development of the security policy. Furthermore, the amount of personal data that could have been compromised due to a breach of information security would be considered for notification purposes, as will be explained later. Although the amount of data compromised is certainly determined in planning the security measures to be implemented, the content of the information will be as well, considered.
2.2.1.2 The synergy of the Information security and Disclosure limitation

Confidential is the quality of that ‘which is done in confidence with the expectation of privacy’, of something ‘private, secret’.\(^\text{15}\) The Disclosure Limitation principle sustains that personal data should not be disclosed only under the data subjects consent or by the ministry of law. Is usually not manifested expressly but rather inferred by reading the provisions rewarding Data Protection.

Expression of what mentioned is to be found in the Article 4(1)(a) of the EPD which establishes that the information should only be accessed by ‘authorized personnel’. The security measures will help to ensure that the principle goal of the disclosure limitation principle is achieved. Processing of personal data must be kept confidential as it is for the best interest of the data subject. Recital 46 of the DPD manifests that security measures have ‘to be taken in protection of the rights and freedoms of the data subjects’.

2.2.1.3 The synergy of the Information security and Data subject participation and control

The data subject participation and control principle is manifested through a combination of rules expressing that a ‘person should be able to participate and have a measure of influence over the processing of data over him by other individual and organizations’.\(^\text{16}\) Information security meets participation and control of data subject especially in the first and second categories of rules as divided by Bygrave.\(^\text{17}\)

The first category of rules is composed by those aiming to give awareness to data subjects about the details of a data process and is mainly manifested in the obligation to provide details of the process to the authorities. The notification of processing to the NDPA, described in Article 19 of the DPD mentions that the security measure should be described to allow its assessment by the authorities.

The second category of rules is manifested in the rules aiming to give awareness to data subjects about the process and its effects on their data. The third subcategory includes ‘rules

\(^{15}\) Statsky (1)

\(^{16}\) Bygrave (n13) 63.

\(^{17}\) Ibid.
requiring data controller to orient data subjects directly about certain information on their
data-processing operations. Data breach notifications could be counted among this type of
rules and represents another example of the synergy between the two principles.

2.2.1.4 The synergy of the Information security and Sensitivity

The Security measures to be taken are affected by the sensitivity of the information to be
processed. The rule of Article 8 of DPD maintains that the processing of sensitive data should
be prohibited, providing as well situation conditions under which such processing could be
allowed. The attention to the sensitiveness of data is a parameter to determinate the
adequacy of the security measures and the seriousness of a data breach.

The processing of sensitive information requires that the security measures have to provide a
higher level of security that in dealing with other kind of information as the risks in case of
data breach are bigger and the nature of the information so demands.

The 29WP in its opinion about personal information gives new guidance respecting
information that even though it is not mentioned as sensitive in the article 8 of the DPD, it still
should be carefully taken care of: bank account, credit card data, credit records, etc.

2.2.1.5 Information quality, Purpose specification

In respect to the other data protection principles as information quality and purpose
specification, the effect of their application over security measures is rather small.

The notions contained in the information quality and purpose specification principles are more
related to process design than related even to the development of a security measures.

---

18 Ibid.


20 Bygrave (n13) 62.

21 Bygrave (n13) 61.
2.3 Information Security Goals

Information security is a ‘holistic system’. The goals mentioned here, though individualized, are in fact parts of a hole. An Information Security system should be aimed at ALL of these goals. Daswani, Kern and Kesavan mention the following goals of security:

• Authentication is the act of verifying someone’s identity to ensure the information can only be accessed by an authorized person.

• Authorization is related to the act of verifying the authority of a particular person related to his capacity to perform certain determinate acts.

• Confidentiality refers to keep the secrecy of information during transfer and storage.

• Data/message integrity, is to be kept. The information should not suffer any alteration by an unauthorized party even if that party does have access to the content of such information.

• Accountability, not only refers to the people responsible within the security system but also in cases involving a breach of security it must be possible to identify who has been responsible for such act.

• Availability, as a security system should be able to give a proper response in a ‘reasonable time frame’.

• Non-repudiation, as every party involved should be able to use the systems meaning that no user should have control over the system to deny the service to other users. Depending on the

---


23 Ibid.

24 Daswani (n22) 7.

25 Daswani (n22) 12.

26 Daswani (n22) 17.

27 Daswani (n22) 18.

28 Daswani (n22) 19.

29 Daswani (n22) 20.
architecture of the system, a trusted third party\textsuperscript{30} could be used to ensure the non-repudiation.\textsuperscript{31}

The “goals” represents the ideal functions and characteristics of a security system. In practice factors as the risk presented by the process, the sensitivity of the information as well as the cost involved on implementation will define how far security can be guaranteed.

The EU legal framework does not provide a full description of the security measures to be implemented. As presented in the DPD, the security measures are not described in detail though considerations for their application are presented. The EPD though, provides a small level of description for a security framework to be applied by organizations in the telecommunication sector. But this description does encapsulate the INFORMATION SECURITY GOALS as will be show next.

The CKD modified the EPD security obligation by introducing a more descriptive information security framework, including express functions that the security measures applied should achieve ‘at least.’\textsuperscript{32} The functions are not to be applied individually as read from text of the Article, which remark once again, the holistic character of information security. The Preventive Security measures have four goals described in the CKD and included in the EPD.\textsuperscript{33} They are basically:

To ensure that personal data can be accessed only by authorised personnel for legally authorized purposes.

To secure the transmission and the storage of personal data; and

To ensure the implementation of a security policy.

\textsuperscript{30} Also known as “Trent”. It refers to software or hardware that making use of protocols, authenticates and authorizes users. For example Kerberos. ‘ Kerberos is a commonly used mechanism for authentication purposes. Kerberos utilises symmetric cryptography as well as public key cryptography, to provide authentication for client server applications... The core of Kerberos architecture is the Key Distribution Centre (KDC). The KDC stores authentication information and uses it to securely authenticate users and services. The KDC acts as a trusted third party in performing these authentication services.’

Y. Kirsal and O. Gemikonakli \textit{An Authentication Protocol to Address the Problem of the Trusted 3rd Party Authentication Protocols} 523.

\textsuperscript{31} Daswani (n22) 21.

\textsuperscript{32} CKD Article 2(4)(b)

\textsuperscript{33} EPD Article 4
The first function is aimed to achieve the Information security goals of Authentication, and Authorization. The second function points at achieving Confidentiality and Data and Message integrity. Finally the implementation of a security policy intends for Accountability, Availability and Non-repudiation to be achieved. As part of a security policy, good practices in case of data breaches should be included. The EPD provides express order to notify the NDPA and the data subject in certain cases of data breaches. More level of detail about information security measures will be provided in the next chapter.

2.4 Risks

Recital 61 of the CKD mentions that

‘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.’

Article 17 of the DPD mentions that the information security measures should protect personal data against ‘accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access... and other unlawful forms of processing.’ First, the text of the Directive mentions that the risks that threaten personal data are loss, alteration, disclosure, access, and other forms of processing, and second, those risks can be of unlawful or accidental nature. Being that disclosure of personal data should be authorized to be lawful, the unauthorized disclosure or access are included in ‘unlawful forms of processing’.

The degree of harm that could affect the data subject depends on how much his privacy is affected by the data breach. For example, unlawful or accidental destruction or loss would have a low effect on the data subject’s privacy. The results that accidental or unlawful alteration of the personal, as in cases of medical identity theft; 34 or the accidental or unlawful disclosure or access to personal data, have a major impact over the data subjects privacy. As this means that other subjects have gain knowledge of the content of the data subject’s personal information.

2.5 Rights and obligation of Data Protection Actors, regarding Information Security

In the process of personal data, the main actors are the data subjects, the controllers and processors; and the Data Protection Authority. During the processing of personal data, the subjects, controllers, processors and NDPAs have rights and obligations to fulfil. Analysing basically the DPD and the EPD, it is found that the data subject – the “weakest” part involved has more rights than obligations, while the bigger obligations have to be fulfilled by the controllers and processors. The NDPAs on the other hand are placed in between the two actors, to provide guidance, to enforce rights and to ensure that obligations are fulfilled. The present analysis will focus on rights and obligation rewarding security measures for the process of personal data.

As occurred with the principles, the rights and obligations of the data protection actors are not always lay down explicitly. Mostly the rights of the data subjects have to be inferred by the other actor’s capacities and responsibilities. The present analysis will take the data subject’s main right as a starting point. Later on it will be contrasted with the obligations placed over the other data protection actors.

Data subjects are natural persons who provide the “raw material” in data processing. Their data is processed, and their privacy placed at stake. The DPD though, does not appoint their consent as necessary for such process to occur as other grounds are appointed on which, the process of personal data is fair and legal.

The 29WP have manifested that ‘reliance on consent to process personal data does not relief the data controller from his obligation to meet the other requirements of the data protection legal framework...’ (Emphasis added). This means that the consent of the data subject to a process of personal data does not excuse the data controller from accomplishing the general obligation of lawfully and fairly processing personal data. The process should observe the conditions stated in the law for to take place, which includes the implementation of security measures. The controller must ‘...implement appropriate technical and organizational measures’ to ensure the integrity of the personal data. This means that a process without appropriate security measure is not be legal.


36 DPD Art 17.
With this in mind, the data subject has the right to demand the implementation of security measures that offer an appropriate level of security from the controller and the processor. Whether the measures provide the appropriate level of security or not, has to be determinated by the NDPA.

In case when the process is entirely or partly automatic, Article 18 of the DPD requires the data controller to notify the NDPA prior starting the process. The NDPA must assess the measures, considering that a description of them should be included in the notification realized by the data controller\(^{37}\) and under the considerations appointed in article 17 of the DPD. The description should allow the NDPA to perform a ‘preliminary assessment’\(^{38}\) about the appropriateness of the level of security offered by the measures.

Data subjects have the right to present claims concerning the protection of their rights and freedoms in regard to the processing of personal data. The NDPA have the obligation to hear claims presented ‘by any person, or by an association representing that person’\(^{39}\). Although is not expected that the data subject have the required level of expertise, in the case he does, it would be possible for him to present claims in relation to the appropriateness of the security level offered by the measures implemented by the Controller.

Article 23 of the DPD defines the rule of liability for controllers and processors, stipulating that ‘any person who suffers damages as a result of an unlawful processing operation... is entitled to receive compensation from the controller for the damage suffered’. The controller has to prove that he is not responsible for the event giving rise to the damage to be exempted of this obligation ‘in whole or in part’. The security measures should provide a level of security in consideration of the points mentioned in Article 4 of the DPD.

Finally, in the case of breach of security that is likely to have compromised personal data, Article 4 of the EPD indicates that the ECSP is obliged to notify the data subjects. The data subject’s right to be notified in cases when his personal data has been likely compromised is under to some conditions that will be explained in further chapters. It needs to be mentioned that the NDPA can decide sometimes whether notification is necessary or not if it has not been already performed.

\(^{37}\) DPD Art 19.

\(^{38}\) DPD Art 28.

\(^{39}\) DPD Art 28.
Recital 61 of the CKD indicates that the notification should allow the data subjects whose data have been compromised ‘to take the necessary precautions’. Though the wording of the recital, implies that the choice should be given to the data subject on whether to take or not precautions, is would only be expected that the measures are taken. For example cancelling credit cards or changing passwords, etc.

To summarise, rewarding the information security provision we find the following rights and obligations.

The data subject has:

- The right to have his personal data processed under an appropriate level of security.
- The right to challenge the appropriateness of the security measures by itself or represented by other person, in case when there is a doubt about their level of security.
- The right to be notified in cases when the security measures have been breached.
- The right to get a compensation for damages derived from a security breach.
- The obligation to take the necessary precautions when a data breach notification has been received.

The National Data Protection Authority has:

- The obligation to assess the appropriateness of the security measures.
- The obligation to hear and resolve the claims from the data subject.
- The right to decide of the convenience of notifying data subjects in cases of data breaches, when such notification has not been performed.

The Data Controller has:

- The obligation to describe the security measures to be implemented in the notification to the NDPA.
- The obligation to improve the security measures when these do not provide an appropriate level of security or when these have been challenged by the data subject and his claim has been accepted by the NDPA.
- The obligation to notify the NDPA in cases of data breaches.
• The obligation to compensate damages suffered by the data subjects, as a consequence of inappropriate implemented security measures.

2.6 Conclusion

As result of the synergy between the information security principle and the other data protection principles, the security measures do more than just provide ‘an appropriate level of security’. They ensure that other goals rewarding the processing of personal data are achieved. Although to keep the safety of the integrity of personal data from being lost or altered and to ensure the confidentiality of the data subject, remain their main objectives. The goals of information security are also influenced by the needs set up through the data protection principles. The information security rights and obligations for the data protection actors derives from the translation of these needs into the text of the EPD. The next chapters will provide a deeper insight of the Information Security provisions as stated in the EPD.
3 Preventive Security Measures

3.1 Overview

The present chapter aims to elucidate the threshold for appropriateness for preventive security measures. Next, a description of how security measures could achieve the information security goals as stated in the EPD will be provided. Finally, the German and Spanish information security provisions will be described, as they might present important examples of possible solutions for the same problems.

The measures analysed in the present chapter have as function to secure the privacy of the data subjects and to guarantee the confidentiality of personal information by preventing the unlawful access to such information in the context of publicly available electronic communication services.

3.2 About the appropriate level of security

The security provisions, as remarked in the previous chapter, are aimed to secure the data process and thus, to ensure that the privacy of the data subject is not adversely affected. The National Data Protection Authority (NDPA) must assess if the level of security offered by the security measures implemented by the controllers are appropriate or not. Article 17 of the DPD indicates that those security measures should ‘ensure a level of security appropriate to the risk represented by the processing and the nature of the data to be protected’\(^{40}\) having regard of ‘the state of the art and the cost of their implementation’.\(^{41}\) When acting in behalf of the controller, the processor must also comply with this obligation, Article 17(2) states that the processor ‘must ensure compliance with those measures’. The terms to describe the security measures are general, but it is clear that the security measures have to be of a technical and organizational nature.

The NDPA have to observe the four elements mentioned in Article 17 of the DPD to assess the level of security granted by the security measures:

- the nature of the information being processed

\(^{40}\) DPD Article 17.

\(^{41}\) Ibid.
The risk represented by the process,
the cost of implementation; and
the state of the art.

The Irish Data Protection Commissioner offers guidance about these considerations as implemented in the Irish legislation. In respect of the nature of the information, the commissioner indicates that the controller, when processing sensitive information, ‘naturally needs to have very robust standards of security in place’ in comparison to a lower standard when processing information ‘with a lower privacy value’.

With respect to the risk imposed by the processing of data, this is in relation to ‘the harm that might result from unauthorised use, disclosure or loss of the personal data.’ In regards to the cost of implementation, the commissioner mentions that ‘if the risks of security breaches are low, and the likely harm that would arise is trivial or minor, then a data controller might justifiably decide not to invest a great deal of money in state-of-the-art security measures.’

The state of the art requires that, ‘security measures need to be reviewed on a regular basis to ensure that they are up-to-date and effective.’ As it can be seen, it is expected from the controllers that the security measures must be kept updated as this is necessary due to new risks that are derived from the constant development of new technology. The obligation to implement information security measures to the processing of personal data varies with time and the constant development of new technologies. The security levels should be maintained in consideration of the new risks and threats posed by such developments. Although, it is not clear how often the NDPA should review the security measures to assess their level of security.

The Regulation to the Spanish Data Protection law (“SDPL”) does provide guidance on this aspect. The SDPL orders the implementation of different levels of security, starting from

---

43 Ibid.
44 Ibid.
45 Ibid.
46 Ibid.
47 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
a ’basic level’ to a ‘high level’ of protection which must to be applied in consideration to the risks represented by the process. The lower the risk is, the lower the necessity to implement a complex information security framework. In its Article 96, the SDPL expresses that starting from the ‘medium level’ security of measures, an audit should be performed at least every two years. In cases where substantial modifications to the information security systems have been undertaken that could affect in the accomplishments of the information security goals, a new audit must be performed.

The BDSG in Section 9(a) states that in order to improve the information security:

‘suppliers of data processing systems and programs, and bodies conducting data processing may have independent and approved experts examine and evaluate their data protection strategy and their technical facilities and may publish the results of this examination.’

The obligation to implement security measures is more specific in the context of telecommunications. Article 4 of the EPD insists that measures should be of technical and organizational nature and lists three goals that the measures should aim at. Also encryption and the notifications in cases of personal data breach are mentioned. We mention this provision to remark that the obligation to implement security measures is clearer in its goals, for organizations of the telecommunication sector than for organizations in other sectors that also process personal data that are subject of the DPD. What is common is that the considerations to be made over security measures to be implemented have to be realized during the stage of design and planning of the process.48

The Irish Data Protection commissioner mentions about the delicate situation regarding telecommunications that:

‘This type of transmission involves particular security risks that must be guarded against. Most obviously, there is the danger that the transmission could be intercepted by a third party. Other risks include corruption or loss of the data, or its accidental disclosure to third parties’.49

The technical and organizational security measures adopted by organizations in the telecommunication sector must at least:

48 DPD Recital 46.
49 Ireland (42).
• Ensure the file is accessed only by authorized personnel and for legally authorized purposes,

• Provide security during transmission and storage,

• And ensure the implementation of a security policy with the respect to personal data.

Although this thesis does not deal with computer science applying to law, some examples of security measures will be given about how the measures indicated at the E-privacy Directive should grant protection during the processing of personal data.

3.2.1 Access and Use limitation

The first function of a security measure is to ‘ensure that personal data can be accessed only by authorized personal for legally authorized purposes’. These two conditions: a) Performed by authorized personnel, and b) For legally authorized purposes, are closely related to the principle of Fair and Lawful processing. Any processing that does not fulfil both conditions should be considered illegal. About its legality, an authorized process being performed by unauthorized personnel and an authorized person performing an unauthorized process will have the same effects. The first case is a form of unauthorized disclosure of personal data while the second case contravene the provisions referring to the purpose specification and the fairness and legality of the processing.

The legally authorized purposes are those that fulfil the criteria mentioned in Article 7 of the DPD ‘for making the data processing legitimate’ and, in special cases, fulfilling as well the conditions for processing sensitive data stated in Article 8 of the DPD.

Focusing on the security of the information, the first function of the protection measure should to limiting the access only to authorized personnel. We can picture the door leading to a big room containing files and data about million people. At first, the security measures should ensure that authorized persons are the only going through that door.

The logic of the security framework based on the authorization of personnel, use schemes that will consider the level of control of the personal to performed a determinated action—Authorization- or in the recognition of the personal authorized —Authentication’, as only authenticated personnel should have access to the process and information. Authorization

---

50 EPD art. 4 (1)(a).
meaning ‘the act of checking whether a user has permission to conduct some action’ while ‘authentication’ refers to ‘the act of verifying someone’s identity’.

The technological framework for limiting access to personal data by means of ‘authorization’, is currently based on the maintenance of ‘Access Control Lists’ (‘ACL’) and ‘Access Control models’ (‘ACM’). The ACL is the information attached to a file about the actions that can be performed by the user over that file. Depending on the influence of the users over the ACL, the ACM applied may vary, though limiting actions to those legally authorized.

As for ‘authentication’ we can mention those based on access cards or other tokens, such as SMART, OPT and ATM cards; schemes based on knowledge, like passwords and codes, or those based on recognition of the biometric information of subjects. Cards and similar objects to grant access will provide security as long as they are kept by the authorized personnel. A password will function while the subject is able to remember it and its secrecy is sustained. The problems that these two methods present are not found in Biometric systems, which ‘couple with a low cost for capturing and processing biometric information, are leading to new applications for biometric every day’.

Security schemes will mostly make use of resources for authorization and verification. For example, transactions via an ATM require the use of the corresponding card and password of the user to verify their identity, while the system will determine the amount of money available, ergo authorizing or not a withdrawal.

---

51 N Daswani (22) 12.
52 N Daswani (22) 7.
53 N Daswani (22) 13.
54 N Daswani (22) 14.
55 D Wright and others, Safeguards in a world of ambient intelligence, 186.
56 N Daswani (22) 8.
57 N Daswani (22) 7.
58 N Daswani (22) 10.
3.2.2 Secure transmission, secure storage

The second goal for security measures in the telecommunication sector is to secure the transmission and the storage of data.\footnote{\text{EPD Article 4(1)(a)}} During transmission the information is vulnerable to be intercepted by a third party to access its content or modify it, affecting its integrity and confidentiality. While during storage, a breach in the information security may carry the same adverse effects.

The first scenario - similar to ‘eavesdropping’ in phone conversations - has been denominated as network eavesdropping. This is regarded as either passive\footnote{\text{N Daswani (22) 18.}} or active\footnote{\text{Ibid.}} depending on whether the eavesdropper has the power to alter the content of the information.

The second scenario is related to any hacking of a databases and the leak of personal information of millions of people that have occurred lately, such as the Sony database breach for example.\footnote{\text{B Quinn and C Arthur, \textit{PlayStation Network hackers access data of 77 million users}, 26 April 2011, http://www.guardian.co.uk/technology/2011/apr/26/playstation-network-hackers-data?intcmp=239 accessed 06 October 2011.}}

External measures, software and good practices can be implemented to reduce the risk of an intruder during the transmission and storage of information. External security measures are for those implemented to protect the servers of a company, like locks, scanners, security posts, cameras and sensors. Software and data will require measures like watermarking, antivirus and firewalls, among others.\footnote{\text{Wright (55) 184.}} Finally, good practices like updates of protection software, detection of changes in hardware configurations and the usage of trusted hardware modules should be performed regularly to ensure a higher level of security to help ensure prevention of data breaches.

Security measures provisions neither promote the use of any particular technology nor advocate for a specific security framework, but the controller can choose to apply the methods that adapt better to the processing of data, its risks and benefits, to reflect what goes on in reality. Both external measures and digital measures should be applied simultaneously. It
is the controller who decides the setup for the security of the processing in conjunction with the considerations of the risk and benefits that such processing raise.

3.2.3 Security policy

The third goal of security measures, as indicated in Article 4 of the EPD, is to ‘ensure the implementation of a security policy with respect to the processing of personal data.’ Accountability, availability and non-repudiation are the goals that should be addressed in the Security Policy.

An Information Security Policy basically constitutes a ‘set of rules defining who is authorized to access what and under which conditions and the criteria under which such authorization is given or cancelled.’ This definition seems short compared to the one proposed by Robert J. Shimonski:

‘A living document that allows an organization and its management team to draw very clear and understandable objectives, goals, rules and formal procedures that help to define the overall security posture and architecture for said organization.

The Policy contains the details about the operation and process related to security at an organizational level.

The functions of the security policy are to:

• Protect people and information

• Set the rules for expected behaviour by users, system administrators, management, and security personnel

• Authorize security personnel to monitor, probe, and investigate

• Define and authorize the consequences of violation

---


• Define the company consensus baseline stance on security

• Help minimize risk; and

• Help track compliance with regulations and legislation.

Furthermore, an ideal security policy must be understandable, realistic, and consistent. The security policy must be stated clearly, documented, distributed, communicated properly and reviewed constantly.  

### 3.2.4 Encryption

Encryption is a function of a cryptographic system; ‘a cryptographic cipher system can hide the actual contents of every message by transforming (enciphering) it before transmission or storage.’ The system makes use of techniques of a mathematical nature and applies it to information security which hides the content of the data or message by replacing its form:

> ‘In cryptographic terminology, the message is called plaintext. Encoding the contents of the message in such a way that its contents cannot be unveiled by outsiders is called encryption. The encrypted message is called the ciphertext. The process of retrieving the plaintext from the ciphertext is called decryption. Encryption and decryption usually make use of a key, and the coding method use this key for both encryption and decryption. Once the plaintext is coded using that key then the decryption can be performed only by knowing the proper key.’  

Being that the proper key should only be at hand of authorized personnel, Encryption in the case of a data breach, will make ‘more difficult to understand the content of stolen data.’ Encryption will help to ensure that the information is only used by certain subjects by ensuring the key for decryption is only at hand for authorized personnel. This characteristic guarantees that the method will provide security during the transmission and storage of the data. Besides this direct effect on the security of the information, Article 4 of the EPD mentions that if the

---

68 Shimonski (66)

69 F Rodríguez-Henríquez and others Cryptographic Algorithms on Reconfigurable Hardware (Springer Science+Business Media, LLC USA 2006) p 8

70 Ibid

71 Supra note 41. 184.
controller proves that encryption, or another method to ‘render the data unintelligible’ has been applied, the NDPA can free the controller from the obligation to notify the data subject.

3.2.5 Security risks warning

At first, a provider must notify the data subject the risks that could rise in connection with a process of personal data in the context of electronic communication services as appointed in paragraph 2 of Article 4 of the EPD.

This “risk warning” must include a description about the dangers the process might carry for subscribers of the service. If the measures implemented, are not capable to provide security against such risks, the ECSP must inform the subscribers about the measures that could be taken to avoid them and eventually, the cost of their implementation. This notification refers to the growing risk of a security breach for a technological change or for a vulnerability being found, in the security implemented. Also, this notification is only meant to reach subscribers of the service, as defined in Article 2(k) of the Directive 2002/21/EC ("Framework Directive"). Meaning that individuals who are not part of the contract, whose privacy might be in risk, will not receive a notification.

3.3 Information Security Provisions in Germany and Spain

Before the CKD was adopted, Germany and Spain had already implemented in their territories, a framework for data protection which included stricter rules for the processing of personal data that the one which until then was available for the rest of data controllers in other member states.

The German BDSG, Section 9 place over ‘public and private bodies which collect, process or use personal data on their own behalf or on behalf of others’ the obligation to take ‘necessary technical and organizational measures’ secure personal information. Indicating that information security measures would only be necessary, ‘if the effort required is in reasonable proportion to the desired purpose of protection.’

The Annex to Section 9, describes eight security goals and five related functions: access control, disclosure control, input control, job control, and availability control.

Access control aims at achieving goals 1 to 3, which include
1) Preventing unauthorized persons from gaining access to data processing systems for processing or using personal data,

2) Prevent data processing systems from being used without authorization, and

3) To ensure that authorized persons have access only to those data they are authorized to access disclosure, and that personal data cannot be read, copied, altered or removed without authorization during its processing, use and record.

Disclosure control aims at goal 4 to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media it is possible to ascertain which bodies are to be transferred personal data.

Goals 2 to 4 in the BDSG, mention the ‘encryption procedures’ as one measure being in ‘accordance’ with such goals, and expressly mention that they have to be the ‘latest’. The Access and disclosure control could be accomplished by implementing encryption technologies. Since the act mentions the latest encryption technologies, it is to be understood, that the Data Controller should try to keep the security measures updated. Input control should ensure achieving the fifth goal, ‘to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom’. Job control relates to goal 6, ‘to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller’s instructions’. Availability control looks to ‘ensure that personal data are protected against accidental destruction or loss’ which is goal 7. Finally, there is no control function specified to achieving the eighth goal which is to ensure that data collected for different purposes can be processed separately.

The German information security framework for personal data is applicable to every organization that processes personal data. The obligation is more specific and clear than its equivalent in the DPD. It also resembles the information security provisions stated in the EPD which only applies to ECSP.

---

72 BDSG Section 9 Annex

73 Ibid

74 Ibid
The SDPL takes on a more complex framework. As mentioned before, security measures are divided in three different levels: Basic, Medium and High. The more risk the processing of personal data implies, the higher the level of the security measures to be implemented.

Article 81 of the SDPL states that the levels of security should be implemented according to the nature of the personal data and includes, as well, that every process should implement the basic information security measures.

The information security measures at the basic level are: the inventory of security incidents, measures to ensure that access to personal data is granted only to authorised personnel only for authorized purposes, measures that allow the identification and authentication of users and security copies and back up information that allow the restore of the information when required. These obligations are described in extensity in their correspondent Articles.

Medium level information security measures include the designation of a responsible of security, an audit of security measures, a registry of access to determined information, a mechanism to avoid unauthorized users from accessing personal data, the control of physical access, an inventory of incidents including a description of the measures taken to restore the data affected.

These measures, and those at the basic level, have to be implemented when processing information relating to administrative or criminal offenses, information on patrimony and credit records, taxes, related to the provision of financial services, social security, work

---

75 SDPL Article 80
76 SDPL Article 90
77 SDPL Article 92
78 SDPL Article 93
79 SDPL Article 94
80 SDPL Article 95
81 SDPL Article 96
82 SDPL Article 97
83 SDPL Article 98
84 SDPL Article 99
85 SDPL Article 100
accidents and diseases, information containing a set of personal data that provide a definition of the characteristics of personality of citizens and allows to assess certain aspects of the personality or their behaviour.\textsuperscript{86}

Information security measures of the High level have to be implemented inclusive of the measures at the basic and medium level when the process refers to personal data relating to: ideology, union membership, religion, creed, race, health or sex life; information containing or referring to data collected for law enforcement purposes without the consent of those affected; data derived from acts of violence against women\textsuperscript{87}. Also, in the context of the electronic communications, service providers have to implement encryption which (is mentioned as a high level measure in Article 103 of the SDPL) to information in traffic and information containing localization data according to the same Article 81.

At the high level of information security measures, the SDPL requires that the controls and registries that are implemented as medium level security measures have a higher level of detail. As it is the case that the registry of access to determined information\textsuperscript{88} which must include more detailed information about the use, date, and identity of the user who accessed or tried to access the information. The backup copy of the information should be kept in a different location from where the data is processed\textsuperscript{89}. Is also required the use of methods that allow the identification of the users, and the information that has been accessed and that prevent unauthorized users from accessing the same data. Encryption should be applied when transferring and storing the data, and the transport unencrypted data in portable devices should be avoided.\textsuperscript{90}

Article 88 of the SDPL mentions that a security policy must be implemented by the data controllers. This document must include a description of the security measures of technical and organizational nature. Furthermore, the document must include a detailed description about its scope of application, the resource to be protected, the norms, procedures, rules and

\textsuperscript{86} SDPL Article 81

\textsuperscript{87} Ibid.

\textsuperscript{88} SDPL Article 103

\textsuperscript{89} SDPL Article 102

\textsuperscript{90} SDPL Article 101
standards to guarantee the highest level of security that were required; and, functions and obligations of the personal in relation to the processing of personal data.

Article 104 requires, among other security measures, that the transmission of personal data in the context of a publicly available electronic communication service will required the implementation of encryption to render the information unintelligible and avoid being accessed by unauthorized parties.

As shown, the German and Spanish law provide a higher level of description regarding the information security measures to be implemented in the processing of personal data, than the provisions in the EPD.

The SDPL eliminates the notion of risk that is present in the DPD and the EPD and implements an objective threshold based on the nature of the information. While this eliminates the shades that could appear while trying to determine the appropriateness of the security measures, it also eliminates other aspects to be considered by an organization and that could allow to reflect the convenience to assume operations of processing personal data, like the cost of implementation.

The BDSG requires a higher level of detail in their information security measures but allows the Data Controller less space for flexibility with its concept of ‘necessity’ that is higher than the threshold of ‘appropriateness’ included in the DPD and the EPD. While the level of description for the information security measures is rather high compared to the directives at the EU level in both jurisdictions, the fact that the frameworks are applicable to every data controller, and not just ECSP, is even more important.

3.4 Conclusion

The measures described in the present chapter have the function to prevent personal data from being compromised. The appropriateness of the information security measures demands an assessment first from the controllers and second from the NDPA (on a case-by-case basis). The German and Spanish legislation reduce the factors which must be taken into consideration when assessing the ‘necessity’ of measures or even eliminates this consideration by including an objective rule. In both cases the security measures are related to the nature of the information.
The use of encryption seems to have gained force as an effective measure to protect the integrity of the information and avoid undesired disclosure. But while this measure gains recognition, other practices are dispersed which can create confusion for controllers operating in diverse Member States. However, it is desirable to mention that a Directive imposing minimum standards is better that a Regulation imposing a higher threshold. This situation which could hinder the Rights of the Data subjects in cases when a Regulation couldn’t keep track of technology.
4 Data breach and Notifications

4.1 Overview

This chapter will develop the notions that surround the notification of personal data breaches as stated in the EPD. Issues like ‘what is a personal data breach’? The trigger for notifications, who should be notified and when, the conditions, content and timing of the notifications will also be discussed. Furthermore, other obligations that arise from personal data breaches will be reviewed.

4.2 Introduction

It has been discussed that a security system is holistic, as insecurity is tackled by different actions, and not just one. In the previous chapter, we described the obligations to implement security measures that apply directly to the processing of personal data in the context of electronic communication services. It was also mentioned that these have a preventive character. The data breach notification regime, however, differs from these measures due to its function as a ‘warning’. It does not have, as goal, to prevent a breach as such from happening, but rather to minimize the potential damage data subjects could face as consequence of a data breach.

The DPD sets out the obligation that all Controllers must implement appropriate ‘technical and organizational measures to protect personal data’.91 These measures should ensure a certain level of security against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.92 The DPD though, does not provide any rule regarding what the controller or the processor should do in case personal information is compromised as a result of a security breach. The DPD only refers to the implementation of security measures.

As mentioned before in section Three, the EPD goes further than the DPD in describing the security measures to be implemented by the providers of publicly available electronic communication services. Among them is the obligation to notify in cases when personal data breach has been, or is suspected that it has been compromised. Let us imagine a fire prevention system. It is not comprised only of smoke detectors, fire extinguishers and fire 

---

91 DPD Article 17

92 Ibid
sprinklers, but an alarm system should also be implemented to warn people of a growing danger of fire.

But what kind of information needs to be jeopardised in order to trigger a notification? When ought the notification from the ECSP reach the data subject by? What should the content of the notification be comprised of? Are there any rights or obligations which ought to derive from these notifications? Who should bear the obligations and rights?

To answer these questions, this chapter will first focus on the concept of a “personal data breach”. Next, the rule concerning the timing for the notification will be analysed. The content of notifications will be explored by comparing different schemes which could be adopted. Finally we will try to elucidate what are the rights and obligations that could arise from a data breach and its notification.

4.2.1 What is a personal data breach?

To answer this question, we must first look to recital 58 of the CKD that makes reference to ‘security incidents that have led to the personal data of individuals being compromised’, while Article 2 (2)(c) of the EPD expands this idea and defines personal data breaches as:

‘...a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community’.

Though a security breach might exist, this does not necessarily imply that personal data has been compromised. The concept of a personal data breach rests on the idea that damage may occur, or have occurred, to the data subject due to misuse of their personal information.

A security breach is commonly defined as ‘an act from outside an organization that bypasses or contravenes security policies, practices, or procedures’, while a ‘security violation’ is an act that has an internal origin as the cause of the breach. An example of a data breach is the

---

93 The business dictionary, meaning of Security Breach  
http://www.businessdictionary.com/definition/security-breach.html (accessed 09 October 2011)

94 The business dictionary, meaning of Security Violation  
http://www.businessdictionary.com/definition/security-violation.html (accessed 09 October 2011)
late security incidents in the Play Station network\textsuperscript{95}, while to illustrate a security violation, we can make use of the stolen laptop with information as a violation of the security instructions to be observed by employees. \textsuperscript{96}

The definition of data breach in the EPD unifies the breach and violation concepts, disregarding the origin of the “breach” and focusing only on the negative effects it carries. No attention is paid to who is responsible of the act, or where the breach is derived from, as the definition of “data breach” in Article 2(h) of the directive states,

“personal data breach” means 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 in connection with the provision of a publicly available electronic communications service in the Community'.

Three conditions have to be fulfilled before a “personal data breach” as presented in the EPD, can be said to have taken place. Firstly, the data breach must occur in the context of a publicly available electronic communication service. Secondly, a security breach or the existence of a significant risk that a data breach has, or could, occur. Thirdly, this breach has caused or may has cause the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data.

In Germany, the data breach term is not used in the Federal Data Protection Act. Section 42(a) refers to personal information that ‘have been unlawfully transferred or otherwise unlawfully disclosed to third parties, threating serious harm to the rights or legitimate interests of data subjects...’ Similarly, the SDPL refers to ‘incidents affecting personal character’. \textsuperscript{97}

The definition of personal data is to be find in Article 2(a) of the DPD, meaning “any information relating to an identified or identifiable natural person”. This definition has been explained extendedly by the 29WP, in its opinion 4/2007. ‘Electronic communications service’ is defined in Article 2(c) of the Framework Directive and refers to usually paid services ‘which consists wholly or mainly in the conveyance of signals on electronic communications networks,


\textsuperscript{97} Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de datos de carácter personal, Artículo 90.
including telecommunications services and transmission services in networks used for broadcasting’ excluding services that provide or exercise editorial control over the content transmitted in the same networks.

The trigger for notification resembles the model used in California\(^9\) as well as other states\(^9\) in the US. This model caused certain rejection from media and scholars, as it was fear that subjects will turn “numb” due to the high numbers of notifications were spread by mediums\(^1\). The fear was shared by Telecommunication’s operators in Europe. The reform that instituted such a regime has been operative since July 2003.

### 4.2.2 Who should be notified?

Article 4(3) of the EPD appoints that in the case of a personal data breach, the ECSP shall notify this event to the NDPA. When it is likely that the personal data or the privacy of the data subject will be affected, a notification must also reach the data subject. This is regardless of whether or not they are a subscriber of the electronic communication service publicly available.

At the European level, the notification must be performed by organizations in the Telecommunication sector that provide publicly available electronic communication services. The UK and Ireland do not depart from this rule, the latter implemented a code of practice that makes it mandatory for organizations that process personal data, in the context of other activities that electronic communications, to notify data subjects when it is likely that their information has been compromised.

Germany and Spain also include the obligation to notify data subjects in cases of data breaches. It pays to mention that both the German and Spanish law are applicable to organizations in the private and the public sector.\(^1\) The BDSG states this obligation in section 42(a). The SDPL establish this obligation in it Article 82, as part of the information security measures at the

---

\(^9\) US California Civil Code § 1798.29.


\(^1\) Schwartz (99) 916.

\(^1\) SDPL Article 2.

BDSG Section 1.
basic level that must be applied by every data controller regardless of the sector in which they operate.

The Californian Civil Code requires that ‘an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified’.\(^\text{102}\) This scope was adopted by Germany and Spain, where organization in public and private sector have the obligation to notify data subjects in case of personal data breach.

Regarding who should be notified, the EPD, requires the notification should only reach the owner of the personal data that has been compromised.

The Irish code of practice also includes the rule that ‘in appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána\(^\text{103}\), financial institutions etc.’\(^\text{104}\)

The UK and Ireland adopted the directive word-by-word, including the definition of ‘data breach’. Though, the latter adopted a scheme of notifications in case of data breach that is applicable to organizations in other sectors,\(^\text{105}\) through the Data Protection Commissioner’s Office.

### 4.2.3 When should a personal data breach be notified?

As mentioned previously, a breach of security that affects personal data being processed and compromises personal data as consequence constitutes a ‘personal data breach’. Every time a security breach involves personal data, a notification to the NDPA from the ECSP is required. When the same personal data breach ‘is likely to adversely affect the personal data or privacy

---

\(^\text{102}\) Section 1789.29

\(^\text{103}\) Ireland’s National Police Service.


\(^\text{105}\) Ireland (104)
of a subscriber or individual... the notification should reach the owner of the compromised data.

The data breach notifications have a warning function: they bring attention of the risk due to the occurrence of a data breach. Therefore, the notifications should be performed in the most expedite manner to allow the data subjects to ‘take the necessary precautions’. The notification requires swiftness in its performance as it has to be delivered to the data subject as soon as the ECSP becomes aware of the data breach.

The Californian Civil Code establishes that the disclosure of the data breach to the data subjects:

‘Shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system’.

The legitimate needs of the law enforcement refer to the effects that the notification might affect with an on-going investigation. Section 1798.82(c) of the Californian Civil Code dictates that the notification shall be performed ‘after the law enforcement agency determines that it will not compromise the investigation.’

The BDSG in section 42(a) mentions that the ‘data subject shall be informed as soon as appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution.’ Article 90 of the SDPL requires only that the notification to be performed and does not expressly provide similar details or comparable points of consideration.

The EPD mentions that the data breach notification should be performed ‘without undue delay’. For some authors ‘without undue delay is a flexible concept allowing for and requiring

---

106 EPD Article 4 (3).
107 Ibid.
108 CKD Recital 61.
109 Section 1798.82.
an evaluation in accordance with the circumstances in each individual case’. 110 There are causes that could prevent the ECSP from notifying the data subject immediately. Expressly mentioned in Article 4 of the EPD, is the notion of the likelihood of adverse effects on the data subject’s privacy.

Recital 61 of the CKD illustrates examples of the ways in which privacy could be adversely affected if a data breach is ‘not addressed in an adequate and timely manner’. It recognises that ‘substantial economic loss and social harm, including identity fraud, to the subscriber or individual concerned’ are some of the dangers and harms which could ensue upon the data subject.

Concerns over the effect that a data breach notification to data subjects might carry over on-going investigations are not laid down expressly in the EPD. Some authors maintain that:

‘in some cases, particularly in criminal investigations, covered entities may have to take into account instructions of law enforcement agencies. Such agencies may require delaying the notification if they perceive that notifying could affect or prevent the criminal investigations’. 111

It is unclear when the ECSP is required to notify other authorities that would be in charge of such an investigation. On the one hand, it might be expected that a warning will be raised and, for example, the police contacted for every time a data breach occurs. While on the other hand, it might be that the ECSP have to consider when that contact has to be taken. The Irish code of practice does mention that in some cases the notification should reach the National Police or financial institutions, 112 although it does not provide guidance regarding when the notification to other law enforcement institutions must be made.

Other point to be taken on account mentioned in other legislations is whether new information security measures have to be implemented prior to notifying the data subject. Article 4(3) regarding the content of the notification to the NDPA mentions that ‘the notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach’.


111 Ibid.

112 Ireland (104).
The fact that the measures could be proposed, or could have already been taken by the ECSP, could indicate that this might not be so relevant when considering notifying the data subject as in the Californian and German legislation. 113

In this respect, Californian Civil Code is clearer than the EPD as it expressly indicates that ‘any delay should not exceed the minimum required to patch the security problem by the swiftest means available.’ 114 Barcelo and Traung mention that, ‘in some cases, it may also be necessary to delay notification until security of the system has been restored’. 115 In line with this last consideration, if there is no confidence that a new data breach could be avoided and no new security measures were implemented, it is unlikely that a notification should proceed until an appropriate level of security is achieved.

If the ECSP has implemented ‘appropriate technological protection measures’ that ‘render the data unintelligible to any person who is not authorised to access it’ (namely, by encryption) there should not be the necessity of notify the data subject 116, as there is not likelihood of adverse affection over the data subject’s privacy.

The Irish Code of Practice in case of Data breach appoints also, that the controllers are exempted of notifying the NDPA in cases when ‘the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or persona data of financial nature.’ 117

In cases where the ECSP has not given the notification, the NDPA can, in regards to the adverse effects that are likely to arise from the data breach, require to the ECSP to notify data subjects. In addition, the authority shall be ‘able to audit whether providers have complied with their notification obligations... and shall impose appropriate sanctions in the event of a failure to do so’. 118 This requirement can be carried out by a law enforcement agency in

113 US California Civil Code § 1798.29. (c).

BDSG Section 42a.

114 Barcelo (110).

115 Ibid.

116 EPD Article 4.

117 Ireland (104).

118 EPD Art. 4
California. Germany treats the failure to notify for a data breach as an administrative offence, with fines up to €300,000.\textsuperscript{119}

4.2.4 Form and content of a data breach notification

Traditionally, a data breach notification has taken the form of a letter. In the EDP, there is no guidance in respect to how a notification could be replaced by other methods of communication that could serve for the same purpose. In particular, the Spanish law does not provide guidance over such matter.

Neither the UK nor Ireland has included any special requirements about the form of the notification to be realized in the NDPA. Ireland however, does include special provisions in the Personal Data Security Breach Code of Practice applicable for organizations outside the Telecom sector in what refers to notifications to the NDPA:

‘Data controller reporting to the Office of the Data Protection Commissioner on accordance with this Code should make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data’.\textsuperscript{120}

The BDSG does make a differentiation in cases when the notification will require a disproportionate effort from the ECSP, ‘in particular due to the large number of persons affected, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying data subjects’.\textsuperscript{121}

More details are provided by the Civil Code of the state of California in section 1798.29, which grants the possibility that, a written or electronic notice could constitute a notification. The possibility of notifying through e-mails, conspicuous posting of the notice on the agency’s web site or through major state-wide media, is available in cases in which ‘the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand

\textsuperscript{119} BDSG Section 43 (2)

\textsuperscript{120} Ireland (104)

\textsuperscript{121} BDSG Section 42a .
dollars ($250,000), or that the affected class of subject persons to be notified exceeds $500,000, or the agency does not have sufficient contact information’.

Furthermore, there is the possibility that an organization uses other methods to notify the data subject when the methods observe the requirements of timing and they are practiced in ‘accordance with its policies in the event of a breach of security of the system’.122

In regards to the content of the notifications, the EPD provides, in Article 4(3), that these should include at least:

- A description of the nature of the personal data breach
- The contact points where more information can be obtained’ and
- Recommendations to mitigate the possible adverse effects of the personal data breach.

The notification to the NDPA will include also the description of the consequences of the data breach and the measures proposed or taken to address the personal data breach.

Nowadays, the Californian Civil Code regarding the notification of a data breach does not have a strong reference about the content of such notification. From January 2012 though, a new senate bill does provide a stronger obligation about this issue.123 The content does not depart much from the required in the EPD, but it add some other information to be communicated in different situations, for example if the notification has been delayed due investigations.

4.2.5 Other obligations arise after a data breach

A data breach not only causes the ECSP to have the obligation to notify the NDPA and data subjects in cases which involve personal data, but it also causes other obligations arise. Other obligations include the obligation to create an inventory of data breaches. Also possible liabilities for the harm that a data subject could suffer can be placed over the ECSP. The obligation to create an inventory of data breaches, should allow the NDPA to audit the performance of the obligation to notify personal data breaches. This inventory is provided for in Article 4(4) of the EPD. The inventory shall include information related to the facts

122 Section 1798.29.

123 SENATE BILL 24 to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal informationhttp://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110819_enrolled.pdf
surrounding the breach, its effects and the remedial action taken. This data ‘shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3,’ which refers to the notification of personal data breaches.

Article 90 of the SDPL, along with the obligation to notify security incidents that involve personal data, include the obligation to maintain an inventory of such incidents. When information security measures of the basic level have been implemented, the information compiled must include the kind of incident which occurred, the time of its occurrence and its detection, the name of the person who is notifying and who was notified, the consequences of such an incident and the measures applied to counteract those effects. Article 100 of the same SDPL states that when a breach occurs while medium level information security measures were implemented, an inventory should also include information regarding the process to restore the information that has been compromised and the person in charge of such process.

In its Personal Data Security Breach Code of Practice the Irish Data Protection Commissioner includes a similar obligation applicable to all data controllers but for those in the Telecommunication sector. The ‘summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data’ should incorporate a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the Office of the Data Protection Commissioner. This information should be provided upon request to the Office of the Irish Data Protection Commissioner.

This obligation is complemented by the ‘necessary investigative powers and resources, including the power to obtain any relevant information they might need to monitor and enforce national provisions adopted pursuant’ that shall have been granted to the ECSP by the member states, according to the EPD. This will allow the NDPA to determine if sanctions should be applied in the cases where the personal data breach notifications have not been performed properly. Article 23 of the EPD states that:

‘Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted

---

124 EPD Article 4(3)
125 Ireland (104).
126 EPD Article 15a (3).
pursuant to this Directive is entitled to receive compensation from the controller for the
damage suffered.’

In cases where the data subject’s privacy has been harmed, or his personal information has
suffered an adverse effect due to a data breach, the data controller can be liable for such
damages under certain circumstances. As it has been previously mentioned, to determine the
fairness and lawfulness of the processing of personal data, the appropriateness of the
information security measures have to be determined. In cases when the data subjects is the
object of harm due to a data breach, the ECSP could be deemed liable whenever it has been
determined that the information security measures implemented did not offer an appropriate
level of security or when the obligation to notify the data subject has not been duly performed.

4.3 Conclusions

A review of the present chapter has indicated that a personal data breach must always be
notified to the NDPA, and reach the data subjects in cases when there is a likelihood that an
adverse effect will harm the data subject’s privacy or their personal information. ‘The issue of
data breach notification is therefore inherently contextual and requires comprehensive case
by case analysis regarding the identification of potential harms and the application of potential remedies’.127 The requirement to notify the data subject is subject to an assessment by the
ECSP, under the conditions that have already been explained above. Once the necessity of
such has been determined, the notification should be performed as swiftly as possible. If not,
the ECSP will risk facing sanctions in cases where such an obligation has not been performed
properly.

Nevertheless, the framework for notification in the case of a personal data breach is far more
complicated than the small explanation presented in the previous Section. The framework is
full of details, highlighting the functions of the notifications, its form, and its threshold for
notification. Still, uncertainties remain not just for the notifications but also for the
information security provisions in general. The next chapter will provide a critical overview of
the current framework of information security provisions with especial attention to data
breach notifications.

127 Burdon, M, ‘Contextualizing the Tensions and Weaknesses of Data Breach Notification and
5 Conclusion and criticism

The development of the functions of the information security measures (prevention and mitigation) as provided in the previous chapters, reveals the evolution that such have suffered through time. This evolution has been produced, due to the needs of individuals and society, in the context of a growing market and technological progress. In a society where information is good highly valued, the needs of the industry could not overrule the data subject’s right to privacy. Information security measures were needed to ensure a framework that could protect this right.

The framework implemented complies with the technology-neutral principle. A framework that incorporates information security measures of different nature (organizational and technological) that as well provides certainty in which goals have to be aimed at. It tries to cover functions of prevention and mitigation as requires the application of information security measures that offer an appropriate level of security while also demands that data subjects be notified in cases of personal data breach. Data breach notification laws ‘also have expansive conceptual aims originated on the conflicting goals of consumer protection and corporate compliance cost minimization’.

The DPD has been implemented by the member states. The examples of Spain, Germany, Ireland and the UK, show the diverse approach that different nations have taken to tackle the issue of providing data subject’s privacy with an appropriate level of security. Germany, the UK and Ireland implemented a more relaxed framework where data controllers could adapt the necessity of implementing security measures considering the cost that such implementation will demand.

For the telecommunication sector, while the UK and Ireland realized a word-by-word implementation of the EPD and the CKD, Germany’s Data Protection Act offered a more descriptive information security framework without neglecting the ECSPs option to adapt the information security to their needs and capabilities. Spain had already implemented an even more descriptive approach without room for considerations, as the level of security to be implemented will vary depending on the kind of information that is to be transmitted. In short, in the EU member states there is not a unify application of the obligation to implement

---

128 Burdon (127) 4.
information security measures. This difference in the implementation of the information security obligation includes to the personal data breach notification obligation.

As described throughout the present thesis, different approaches have been taken about the notification in cases of personal data breaches in the mentioned countries. The difference in the implementation of the personal data breach notification obligation is easy to highlight. If we compare the set of the obligation in California, with the adoption in countries like Spain and Germany and the implementation in UK and Ireland, the variants are quite remarkable.

There is certainly a need to unify the threshold for notification and clarify the criteria to assess the necessity of notifying the Data Subject, as this is a critical issue. Especially in situations where an ECSP has operations in several member states, and is required to deal with laws with different settings.

The Vice-President of the European Commission has expressed her intentions to extend the personal data breach notification obligation to controllers in other sectors. The 29WP has also expressed that steps should be taken to encourage the application of such practice. If such reforms were implemented, other institutions like hospitals and banks will have the formal obligation to notify data subjects in cases of personal data breach. While such obligation is already extensive to data controllers in countries like Spain, Germany, or Ireland.

To extend the obligation to notify data subjects in cases of personal data breach will require that the threshold for notification will be clarified in a higher degree. The data controller should be allowed to perform a better assessment of the need of performing a notification to ensure that notifications only reach the data subjects when strictly necessary.

Though there exists an obligation to notify the data subjects, the rules about data controllers liability, are rarely applied. As it difficult to proof the relation between the harm suffered by a data subject and a personal data breach. The US Laires Insitute issued in July 2011 a study

---

129 Viviane Reading, Vice-President of the European Commission, EU Justice Commissioner, London, 20 June 2011: ‘I intend to introduce a mandatory requirement to notify data security breaches – the same as I did for telecoms and internet access when I was Telecoms Commissioner, but this time for all sectors, including banking and financial services’.

130 ‘Pending a review to be carried out by the Commission of all relevant Community legislation in this field, the Commission, in consultation with the European Data Protection Supervisor, should take appropriate steps without delay to encourage the application throughout the Community of the principles embodied in the data breach notification rules contained in Directive 2002/58/EC (Directive on privacy and electronic communications), regardless of the sector, or the type, of data concerned.’
called ‘Data Breaches and the Phantom Damage Allegation’. The study review the application of law that had been performed in the American courts in cases of allegations of damages which derivate from Data Breaches. The key finding were that the courts were not granting damages in cases were a mere expectation of suffering harm was the cause to filled the complaint and that in most cases, the data subjects were not able to relate the damage to an specific data breach, satisfactorily especially in cases were several data breach notifications were received.

We have already mention that determining the effect that extending the obligation to notify data breaches will have on the amount of notifications to be emitted, is not possible. Nevertheless, the Commission must consider this, to prevent as well that the amount of notification will hinder the possibility for data subjects to receive reparation of the damages suffered as cause of a personal data breach.

Different reports show that during the last few years, cases involving security issues have diminished but levels are still far away from showing a 100 per cent safe status. These results are consequence of the conjunction of diverse factors. Better technology, data controllers more aware of the costs that a personal data breach carries (both monetary and in reputational), and the dissemination of good practices among data subjects. Security as holistic system requires several actions to tackle insecurity. If Data Controllers and NDPA are willing to benefit the protection of the right to privacy of data subjects it is necessary that the data subjects are included into the development of policies and practices, whether as individuals or trough civil rights organizations, as only concurrent actions will ultimately provide the highest rate of success.

131 Lares Institute ‘Data Breaches and the Phantom Damage Allegation’
http://op.bna.com/pl.nsf/id/dapn-8jsjtx/$File/lares.pdf (05 September 2011)

6 Bibliography

6.1 Books


S Gutwirth and others *Data Protection in a Profiled World* (Springer Science+Business Media B.V. Dordrecht 2010)

F Rodríguez-Henríquez and others *Cryptographic Algorithms on Reconfigurable Hardware* ( Springer Science+Business Media, LLC USA 2006)


6.2 Articles


6.3 Legislation

EUROPEAN UNION

Directive 95/46/EC of the European Parliament and 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


USA

California BILL NUMBER SB 1386 to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information. FEBRUARY 12, 2002

California SENATE BILL 24 to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110819_enrolled.pdf

Texas H.B.ANo.A300 AN ACT relating to the privacy of protected health information; providing administrative, civil, and criminal penalties.

SPAIN

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, (Data Protection Law)

GERMANY


IRELAND


UNITED KINGDOM


6.4 Opinions

Article 29 Working Party Opinion (EC) 15/2011 on the definition of consent, 13 July 2011


6.5 Websites


OECD, Guidelines on the protection of Privacy and Transborder flows of personal data, http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html (05 October 2011)


6.6 Speaches

Viviane Reading, Vice-President of the European Commission, EU Justice Commissioner, London, 20 June 2011