

# Forensic Breach Response in Compliance with GDPR

MADELEINE SERENHOV

MASTER'S THESIS

DEPARTMENT OF ELECTRICAL AND INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING | LTH | LUND UNIVERSITY



# Forensic Breach Response in Compliance with GDPR

Madeleine Serenhov  
madeleine@serenhov.com

Department of Electrical and Information Technology  
Lund University

Supervisor: Paul Stankovski

Examiner: Thomas Johansson

February 18, 2018



---

# Table of Contents

---

0.1	Acknowledgements . . . . .	v
0.2	List of acronyms . . . . .	vi
0.3	Definitions . . . . .	vii
<b>1</b>	<b>Introduction</b> . . . . .	<b>1</b>
1.1	Background and motivation . . . . .	1
1.2	Purpose . . . . .	2
1.3	Problem statement . . . . .	2
1.4	Limitations . . . . .	3
1.5	Outline . . . . .	3
<b>2</b>	<b>Approach and Methodology</b> . . . . .	<b>5</b>
2.1	Research strategy . . . . .	5
2.2	Literature study . . . . .	7
2.3	Collection of data . . . . .	7
2.3.1	Interviews at Knowit . . . . .	8
2.3.2	Interview at fintech company . . . . .	8
2.3.3	Forensic observation . . . . .	9
2.4	Conclusion . . . . .	9
<b>3</b>	<b>Theory</b> . . . . .	<b>11</b>
3.1	GDPR . . . . .	11
3.1.1	Roles and responsibilities . . . . .	13
3.1.2	Personal information . . . . .	14
3.1.3	Sensitive personal information . . . . .	14
3.2	Breach response . . . . .	15
3.3	Incident management . . . . .	15
3.4	Computer forensics . . . . .	16
3.5	Information security . . . . .	17
3.6	Laws, regulations and standards . . . . .	17
3.6.1	PUL and MSB - Current instance for incident reporting . . . . .	18
3.6.2	ISO 27000 family . . . . .	18
3.6.3	NIS . . . . .	18
3.6.4	PCI DSS . . . . .	19
3.6.5	NIST . . . . .	20

3.7	Attacks and Intrusions . . . . .	21
3.8	Logs and log storage . . . . .	21
3.9	Recent incidents . . . . .	23
<b>4</b>	<b>Empirics</b> _____	<b>25</b>
4.1	Interviews . . . . .	25
4.2	Observations at fintech company . . . . .	27
4.3	Forensic investigation . . . . .	27
<b>5</b>	<b>Results</b> _____	<b>29</b>
5.1	Clarification of GDPR . . . . .	29
5.1.1	Article 33 . . . . .	29
5.1.2	No subject at risk . . . . .	30
5.1.3	Subject at risk . . . . .	31
5.2	Forensic investigation . . . . .	33
5.2.1	The forensic alteration . . . . .	33
5.2.2	Intrusion points . . . . .	34
5.2.3	Logs and log storage . . . . .	36
5.3	Incident management . . . . .	37
<b>6</b>	<b>Discussion</b> _____	<b>41</b>
6.1	Engagement from top-management . . . . .	41
6.2	How private is private data? . . . . .	41
6.3	The impact of GDPR . . . . .	42
6.3.1	Reporting . . . . .	42
6.3.2	Data erasure . . . . .	43
6.3.3	Time aspects . . . . .	43
6.4	Breaches . . . . .	43
<b>7</b>	<b>Conclusion</b> _____	<b>45</b>
7.1	Summary . . . . .	47
<b>8</b>	<b>Future work</b> _____	<b>49</b>
	<b>References</b> _____	<b>51</b>
<b>A</b>	<b>GDPR Article 4 – Definitions</b> _____	<b>55</b>
<b>B</b>	<b>GDPR Article 33</b> _____	<b>57</b>
<b>C</b>	<b>GDPR Article 34</b> _____	<b>59</b>
<b>D</b>	<b>Recital 86</b> _____	<b>61</b>
<b>E</b>	<b>Questions for qualitative interview</b> _____	<b>63</b>

---

# Abstract

---

Modifications and new approaches for *breach response* and forensic investigations for compliance with the General Data Protection Regulation, GDPR, is to be expected in May 2018. This paper brings forth the conclusion that engagement from top management is crucial in order to comply with the GDPR requirements. The importance of having a vision and a strategy assessing the matters of *breach response*, so that resources can enable procedures for an investigation, is articulated. To enable appropriate countermeasures, a clear understanding of the regulation is essential and presented in terms of severity of *risk to the rights and freedoms* of an individual. Including required actions to take upon a breach and the time-frame of each obligation. Furthermore, the report discusses an approach to approximate the number of individuals being affected by a breach, through looking at the *intrusion point*. This is an essential step since every incident report that needs to be communicated to Datainspektionen needs to assess the approximate number of individuals affected. Assessing the effects of an incident through the *intrusion point*-approach, is an initial step before the forensic analyst may define the exact number of affected individuals.



## 0.1 Acknowledgements

This Master's thesis has relied on valuable input and guidance from the employees of Knowit Secure and the supervisor Paul Stankovski at Lund University. A special thanks to the thesis supervisor from Knowit, Gustav Nordenskjöld, as well as to Åsa Schwarz and Freja Westerlund for their help and provision of ideas.



## 0.2 List of acronyms

AAA	Authentication, Authorization, Accounting
BCP	Business Continuity Plan
CIA	Confidentiality, Integrity, Availability
CIRT	Computer Incident Response Team
DLP	Data Loss Prevention
DPIA	Data Privacy Impact Assessments
DRP	Disaster Recovery Plan
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IDPS	Intrusion Detection/Prevention System
IPS	Intrusion Prevention System
ISMS	Information Security Management Systems
LIS	Ledningssystem för informationssäkerhet
MSB	Myndigheten för samhällsskydd och beredskap
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PII	Personal Identifiable Information
PUL	Personuppgiftslagen
SIEM	Security Information and Event Management

## 0.3 Definitions

Breach notification	The conducted procedure of notifying a party of a breach
Breach response	The procedures of actions to take upon a breach to mitigate the damage caused and reduce the risk of unauthorized data access.
Consent	The permission given by an individual for its data to be stored
Containment	Narrowing down the scope of a breach and minimizing the effect on neighboring systems
Compromised data	Data that has been exposed, altered or liable to danger
Data subject	The individual who is the subject of personal data
Data object	The records linked to the data subject
Intrusion point	The part of a system where an attack is initiated
Recitals	Causes/reasons that the articles in GDPR are built upon
State of the art	Highest level of general development.



---

# Introduction

---

The new European General Data Protection Regulation, GDPR, is coming into effect in May 2018. At the time of writing (January 2018), the effect on corporate organizations and companies is substantial and should be carefully assessed as to not create unwanted implications. The regulation restricts companies and organizations from collecting more data than *what is relevant in relation to the purposes for which they are processed*. All data containing personal information about an individual, here to be called data subject, will require said individuals' consent. The *rights and freedoms* of the data subject are to be protected, but the implications for entities processing personal data shall not be neglected [1]. Strict requirements on actions to be taken upon a personal data breach are stated in GDPR, covering notification to *national supervisory authority* as well as to the individuals affected by the breach. The denominator of GDPR, forensics and breach response is the *Personal Identifiable Information*, PII. PII is the core of GDPR, and breach response, with forensics as a tool, is the procedure of assessing which PII that have been affected by a potential breach. This thesis will investigate the adoption of new and altered obligations in incident response and establish guidance in accordance with GDPR on how to conduct the procedures for breach notification.

## 1.1 Background and motivation

Data breaches are becoming part of our daily lives. Companies more frequently than ever before are admitting to having breaches in their systems. GDPR is a regulation that brings light to the matter in various ways through forcing affected companies to go public with their issues and act upon it. A data breach may result in millions of private personal records and sensitive data being exposed. *Compromised data* is a subject that now has caught the public's attention, leading to the question, is GDPR here to make companies pay for their mistakes?

In 2012 the European Commission proposed a comprehensive reform of data protecting rules in the EU. In 2016, GDPR was accepted with the objective to give citizens back control over their data. GDPR declares how organizations, authorities and other entities are allowed to collect and use personal data within the EU [2]. This enforces every data collecting entity to go over their current IT security and likely adopt changes. GDPR is expected to have a large impact

on the way organizations handle data containing personal information. Prior to GDPR, there was little to no legal framework that provided requirements on how to handle data concerning individual's personal information with as much care. Hence, the GDPR areas that so far have been in the spotlight are the requirements to enable the possibility of *data erasure*, *data portability*, and *consent*, as opposed to *breach response* that very recently has raised concerns. *Breach response* covers the actions to take upon a breach, including notifying data subjects and reporting to supervisory authority. Examples of areas that need to be investigated before an organization will know how to take the correct measurements are, when breach reporting needs to be done, what information that needs to be reported and to whom, how to obtain the information to report and how to get the e-evidence to prove that the report is truthful. In order to be compliant with the new regulation, these steps towards a breach response plan are essential. It includes being able to distinguish whether a personal data breach has taken place, followed by taking the subsequent steps to avoid the sanctions that may be applicable if failure to follow the requirements take place.

To conclude, GDPR puts Personal Identifiable Information, PII, in focus, which, while exposed, executes the breach response plan which needs to be established and accurate.

## 1.2 Purpose

To enhance the knowledge in the field, this thesis goal is to examine breach response in order to be compliant with GDPR, and what preventive measures that need to be in place. The chosen topic is found to bring value due to the still unexplored area and to be of relevance for all organizations affected by the GDPR, all organizations processing personal identifiable information.

## 1.3 Problem statement

The main problem this thesis will investigate is how forensic methods and preventive measures must be adopted to handle the new requirements of breach response in GDPR. This problem statement is broken down into three subareas:

1. **Clarification of the regulation** - What needs to be reported and to whom?
2. **Forensic investigation** - How to obtain the requested information to be reported. E.g. how to narrow down the scope of a breach to not assume all subjects in a database have leaked.
3. **Incident management** - Investigate methods and processes of incident management in order to provide best possible environment for forensic analyses.

These three subareas will be discussed in the above-mentioned order. In the conclusion presented in Chapter 7, recommended approaches to all three subtopics will be presented.

## 1.4 Limitations

This section presents the limitations of scope taken and the present state of GDPR.

The national supervisory authority, that has the power to adopt the regulation in Sweden, is Datainspektionen. An investigation of how the regulation shall be adopted in Sweden is currently in progress. SOU 2017:39 is the complementary regulation from May 2017 that has been under *submission of comment* and was presented in December 2017, together with the legislative proposal [3]. Data Protection Working Party 29 has published their guidelines on Personal data breach notification, adopted on October 3. No further guidance has been published at this stage. This is of relevance since the regulation is not yet in action and might likely be provided with further guidelines from Datainspektionen and the national government on certain paragraphs which today are vague to the reader.

Within GDPR, limitations have been made to not go into detail on the entire procedure of incident management. The scope has been narrowed down to the preventive measures and guidance of breach response, including aspects of forensic analyses. Primarily the Articles 33-35 of GDPR, covering breach response, will be examined. However, this thesis will not conflict nor ignore the rest of the regulation.

Limitations have also been made to not examine how to evaluate the degree of risk of a breach. Whether it is an immediate risk, high risk, risk or no risk, to the rights and freedoms of a natural person.

Security software such as Intrusion Detection Systems, IDS, Intrusion Prevention Systems, IPS, and Security Information and Event Management software, SIEM, will not be evaluated, but are considered to be of interest and relevant to detecting malicious activity and supporting incident response efforts.

## 1.5 Outline

A concise account of *Methods* is conducted in Chapter 2, where chosen approaches adopted for this thesis are presented and explained. This chapter also presents the two sections of collections, (1) Literature study and (2) Data collection, that will be assessed in Chapter 3 and 4, respectively. Chapter 3 presents relevant theory and concepts, covering the regulation GDPR itself together with other regulations that we may learn from, as well as definitions of certain concepts of importance. The theory is followed by the *empirics* in Chapter 4, which covers the performed interviews and observations leading on to the *Result* in Chapter 5. Chapter 5 merge the empirics with the theory and allows for a conclusion based on both facts and observations responding to the three subareas that are presented in the *Problem Statement*. The results will be discussed in Chapter 6, *Discussion*, and the thesis is finally concluded in Chapter 7, *Conclusion*. Appendix A contains several definitions of GDPR-concepts, taken from the GDPR Article 4. Article 33 and Article 34 can be found in Appendix B and C, respectively. Recital 86 of the GDPR is in Appendix D, and finally, questions for qualitative interview in Appendix E.



---

# Approach and Methodology

---

In order to gain a sufficient foundation to draw conclusions from, a good understanding of how incident management and breach response is being performed today, and what changes in that specific scope that needs to be altered to comply with GDPR, is necessary. For this, a qualitative and iterative research approach has been adopted. This approach is considered suitable for investigating the impact of this new regulation due to the incomplete adaption to Swedish law. This enables room for change of interpretation of the articles of GDPR which lays ground for the need of a flexible approach. This chapter presents the chosen methods and why they were implemented. The first two sections cover the decision of qualitative and iterative research, the definitions and how they are adopted in this thesis. The following three sections cover the literature study and collection of data. The Literature study is presented in Chapter 3, Theory, and Chapter 4 is the operational collection of data through interviews and observations.

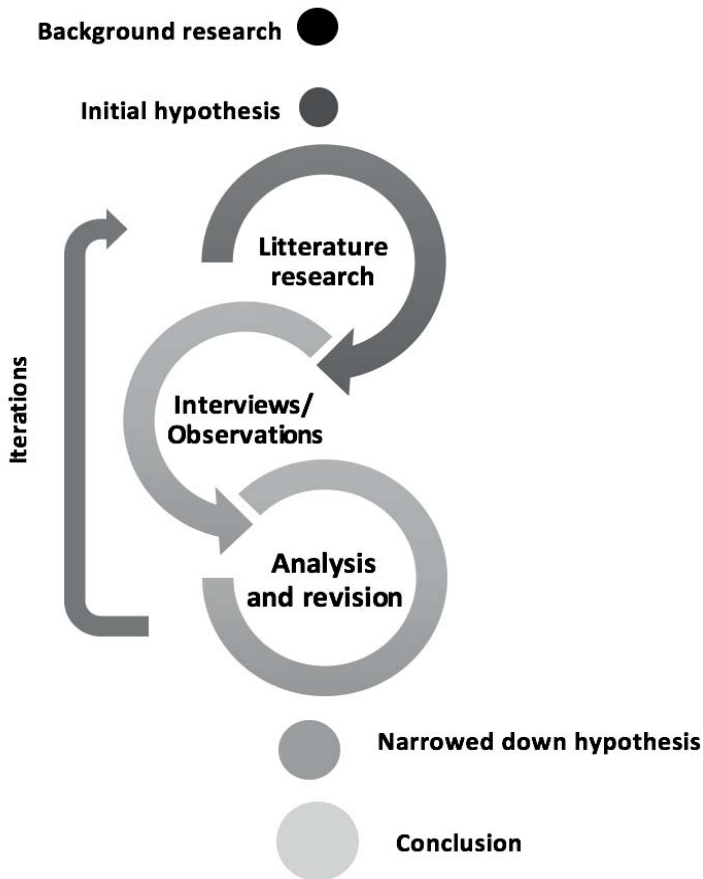
## 2.1 Research strategy

This section introduces the reasons for the chosen qualitative research, as opposed to a quantitative one. Both will be outlined and explained. This section will also present the iterative approach used in addition to the qualitative research.

The fundamentals of a qualitative research are to gain an understanding of underlying reasons, opinions and motivations, in this thesis, in regards to breach response. This has been relevant due to the initial uncertainty of how these questions have been approached before. The qualitative approach is an exploratory way of research that provide insights into problems through techniques such as *unstructured* and *semi-structured* data collection. The research usually involves groups of small sizes and could be focus groups, individual interviews or observations [4]. A *Quantitative research* would, on the other hand, bring forth statistical results and other means of quantification. This would be hard to adopt to this specific thesis due to the inflexible result. Quantitative research often uses large samples and numerical statistics. It would not be possible to obtain as much valuable information from a survey generating numerical values as from the open-ended discussions taken in the qualitative research. The qualitative research has therefore been chosen to give a flexible approach using open-ended questions and discussions.



The chosen iterative approach consist of three primary parts, (1) the literature research where the legal parts of GDPR and other regulations and standards will be examined, (2) observations and interviews to get a rich and holistic understanding of today's situation, and (3) analysis and revision, to then restart again. Prior to the iterations, a background research was performed followed by defining an initial hypothesis, as shown in Figure 1. Finalizing all iterations, the approach closes with a narrowed down hypothesis and a final conclusion.



*Figure 1 Iterative process of the adopted research method.*

Existing assumptions on GDPR-interpretations and breach response, gained from the early literature research and in interviews, were explored and discussed. At the *analysis and revision* stage, the focus gradually shifted from the initial approach of investigating optimal forensic methods, to tracing the problem up to the steering-committee. This, through the obtained understanding of the importance and impact of enclosing processes and methods. From the new knowledge and guiding values, processes such as steering documents and disaster recovery plans

were looked into. After each iteration of new insights and revised assumptions, the hypotheses could be revised and finally be broken down into the three main questions that earlier were presented in the Problem Statement as the *narrowed down hypothesis*.

## 2.2 Literature study

The examined literature has been laws, legal documentation/regulations, standards and guidelines. These papers, given out by well-known global organizations and institutes, are considered to be well-established sources of information. Accurate guidance in both GDPR and incident management is of great importance. Guidance has therefore been emphasized through the chosen literature.

Initially, relevant parts of the GDPR have been read together with associated *recitals* followed by the Swedish interpretation of the regulation. Datainspektionen continuously produces material and guidance for facilitating the compliance with GDPR for organizations and shares their understanding on the Swedish adaption. Therefore it has been necessary to be up to date with the new papers that have been given out throughout the entire process of writing. Article 29 Working party, WP29, is an independent European advisory body on data protection and privacy that has conducted papers on their understanding of the regulation. WP29 has been used in this paper as a great source for accurate interpretation on several articles of the regulation.

Furthermore, additional regulations covering breach response have been examined, such as the Payment Card Industry Data Security Standard, PCI DSS [5]. PCI DSS already has requirements for log management and methods for analyzing an intrusion, which goes much deeper than the guidance of GDPR. Unlike GDPR, the PCI is not focusing on personal data, but rather on card data, which will be looked into to see if the same procedures will be possible to adapt. PCI DSS is a good starting point since it is an in-depth and well established standard with similar principles.

Finally, organizations such as NIST, ISO and OWASP have several relevant papers on guidance and *state of the art* procedures within incident management that have brought great value to this paper.

## 2.3 Collection of data

Empiric studies have been conducted through several qualitative interviews at Knowit together with one deeper *semistructured interview* at a client of Knowit, finalizing with a forensic investigation. Below, the two types of interviews will be examined together with the reasons and definitions of the chosen types, as well as the forensic investigation. The final collection of the data is presented in the Empirics in Chapter 4.

### 2.3.1 Interviews at Knowit

As this master thesis is conducted at the consulting-firm Knowit Secure, nine interviewees have been consultants of the firm. Knowit Secure is a leading security firm in the Nordics and known for its both broad and deep competence with over 15 years in the field for the majority of the consultants. Two interviews at the connected firm Knowit Digital Law have also been conducted for the legal aspects of GDPR. The goal of these interviews was to (1) Get an understanding of the current situation in the field (2) Get input and their understanding of the problem statement (3) Get a correct understanding of GDPR. The following categories of employees have been interviewed;

- Knowit Secure
  - 3 Senior Management consultants
  - 2 Security consultants
  - 1 Penetration tester
  - 1 Information security expert
  - 1 Security specialist
  - 1 Top management
- Knowit Digital Law
  - 1 Digital law consultant
  - 1 Top management

The interviews have been in the shape of both *informal* and *unstructured* interviews. Depending on the employee's position, role, and background, a particular query strategy has been used in combination with an open discussion. The benefit of *informal interviews* is that the respondent may just see it as conversation and may, therefore, foster low-pressure interactions and speak more freely, which helps to gain a good understanding of the area. *Unstructured interviews* tend on the other hand to still be open-ended but express a little more control. There is a clear plan regarding the focus and goal of the interview which guides the discussion [6]. The time for each interview has ranged from 30 min up to 3 hours, depending on relevance. A disadvantage with open interviews is that it's hard to make statistical conclusions and graphs from the result. Since those types of result not would bring much value to this specific thesis, they have not been applied.

### 2.3.2 Interview at fintech company

Two sessions of *semistructured* meetings took place at a client to Knowit. The interview/observation was conducted with the Chief Information Security Officer at a fintech company. *Semistructured* is a common type of interview within a qualitative research approach. The interview is open, based on a framework of themes to be explored allowing new ideas to be brought up as a result of finding new interesting paths. The interview gave a complementary verification of a typical situation of an organization's information security measures. Questions discussed can be

found in Appendix E. The second phase was partaking in a meeting discussing compliance and creation of Business Continuity Plan, BCP, for the company. A general knowledge of how different security procedures work, was gained.

### 2.3.3 Forensic observation

To get a better understanding of how a forensic investigation works, a case of an incident at a client got analyzed and investigated together with an employee from Knowit. This included all steps from making the hard drive copy to writing the report. The investigation is further presented in Chapter 4.

## 2.4 Conclusion

Concluding this chapter, literature with primary sources from the European Union Commerce, Swedish laws and widely known and established frameworks on information security such as the ISO and NIST frameworks have been used. As the second source of information, in this paper called empirics, open ended interviews have been conducted with security consultants and one CISO as well as one performed forensic investigation. A qualitative and iterative approach has been chosen as the most suitable tools/methods for investigating the proposed problem statement.

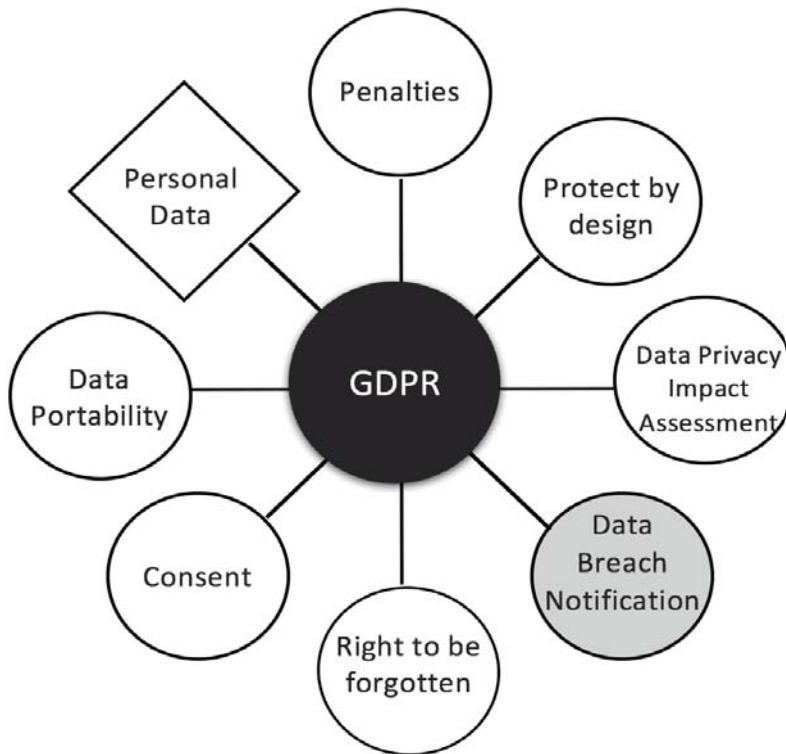


In this chapter the theoretical literature studies are presented. Relevant concepts are defined and explained together with legal terms. Each section covers a new term or theme that will be of relevance for the result and discussion. Firstly GDPR will be examined in general, the specific articles of importance, additional laws followed by incident management, common attacks and recent intrusions.

### 3.1 GDPR

The GDPR will apply from 25 May 2018 when PUL, the current Swedish privacy protection law, will be abolished. GDPR was adopted by the European Parliament and will be directly applicable in every EU Member State and carries considerably tougher sanctions than current legislation. If processing of personal data is not done in accordance with the legal framework, a fine of up to 4% of a company's global annual sales, or 20 million Euro, depending on the higher one, may be applicable. Any company working with information relating to EU citizens will have to comply with the requirements. The regulation consists of 99 articles and 173 recitals. The recitals are underlying reasons that the articles are built upon. Each article is linked to on one or more recitals [7].

The regulation aims to protect fundamental rights and freedoms of natural persons, and in particular the right to protection of personal data. Several areas are covered by the GDPR, but all with the core in PII, as illustrated in Figure 2. Such as the right to be erased and forgotten, and also the right to request data portability and clear consent for processing personal data. GDPR also restricts companies and organizations from storing personal data for longer time than necessary, prohibiting storage of data that is not relevant for the business and enforce penalties if not done accordingly [8]. Article 83 expresses that the competent supervisory authority will make an assessment “in each individual case” when deciding whether to impose an administrative fine [9]. Data breach notification, enforced in Article 33 (Appendix B), is the part of the regulation which will be the focus of this paper.



*Figure 2 The scope and focus of GDPR, with emphasize on Personal Data as a central part and Data Breach Notification as the focus of this thesis.*

In accordance with GDPR, a breach must be communicated to the supervisory authority within 72 hours after having become aware of the breach, and affected individuals have to be notified if the severity so requires. The first paragraph of Article 33 states the following:

*"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay." [10]*

An additional article of relevance is Article 34, please see Appendix C for the entire article. This article describes when the personal data beach has to be communicated to the data subject. Its first paragraph requires the controller to communicate the breach to the data subject without undue delay, cited as:

*"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall com-*

*communicate the personal data breach to the data subject without undue delay." [11]*

Paragraph 3 on the other hand announces that communication to the data subject should not be required if it would involve disproportionate amount of effort or if the breached data was encrypted or unintelligible. Article 34, relative Article 33, requires the risk to be "high" for triggering the communication to data subjects in contrast to communicating to the supervisory authority where the risk does not need to be "high", just being a risk. This means that each degree of risk triggers different escalation points and subsequent obligations. Recital 86, Appendix D gives further information on this.

To be able to minimize risks to data subjects the GDPR requires, in Article 35, data controllers to conduct Data Privacy Impact Assessments, DPIAs, where infringement of subjects privacy is high.

*"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks." [12]*

The DPIA is to be performed prior to collection and processing and assess the potential risk that could result from a breach. DPIA is enforced to mitigate a breach and create awareness.

To conclude, breach notification requires notification to the supervisory authority within 72 hours as well as potential notification to affected individuals depending on severity.

### 3.1.1 Roles and responsibilities

GDPR calls for the mandatory appointment of specific roles. These are new for some organizations, old for others. Three fundamental roles in regard to breach response are *Data Controller*, *Data Processor* and the *Data Protection Officer*. The definitions of the terms have not been altered in GDPR, only their responsibilities and obligations.

#### Data Controller

A data controller is a key person in breach response. The controller decides whether or not a breach has reached a trigger point, of subject being at risk, and an incident needs to be escalated. Escalation involves notification to both the supervisory authority and data subject, if needed. Article 4 defines the role as:

*" 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" [13]*



## Data Processor

On behalf of the controller, the *data processor entity* processes data in accordance with a given framework. The framework, conducted by the controller, defines the purpose of processing and how it shall be performed. The processor has to demonstrate compliance with the given framework, as well as with GDPR. The processor has obligations to alert the controller of any sign of a breach without undue delay after having become aware of it. Article 4 defines the role as:

*"'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[13]*

## Data Protection Officer

The Data Protection Officer, DPO, is the point of contact for all regulatory oversight agencies. Its contact details should be published publicly, be easily accessible and also be included in the report to the supervisory authority upon a breach. The DPO could be a controller or processor's staff member.

### 3.1.2 Personal information

It is important to differentiate data processing between personal data and sensitive personal data, to be able to incorporate adequate security measurements. The terms have previously not been as broad, but as of article 4 in GDPR, personal data is considered to be:

*"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[13]*

This means that by stating "natural person" the scope of GDPR is limited to only cover PII of people who is alive. However, basically any information that one may have about someone is considered to be personal data as long as it, in some way, is possible to identify a natural person from the information. Examples of personal data may be: name, address, telephone number, identity number, email, photos but also license number, IP-address and cookies.

### 3.1.3 Sensitive personal information

Stronger grounds need to exist for processing sensitive data, it is by default prohibited through Article 9. The article defines sensitive data as:

*"Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life."[14]*

PII and sensitive PII is something that GDPR does differentiate between during the incident management procedure, as different actions are required to be taken depending on severity [14].

## 3.2 Breach response

A *data breach* occurs when a data source successfully gets infiltrated and sensitive data manage to be extracted. Moreover, a personal data breach, according to Article 4 in GDPR, is considered to be:

*“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”* [13]

This, in contrast to a *security incident*, solely focuses on data breaches concerning personal data. A data breach can be categorized into the security principles defined by the CIA triad, Confidentiality, Integrity and Availability (explained in Section 3.6) depending on whether it regards a disclosure, loss of access/alteration or stolen personal data. A personal data breach sums up to be any kind of unwanted procedure performed on personal data.

*Breach response* is about preventing, reacting and addressing a breach, minimizing the damage, identifying the issue and efficiently communicating the issue through *breach notification procedures*. *Breach notification* has to be performed internally as well as to the general public so that they may take measures to protect themselves from financial fraud, identity theft, or other personal injury [15]. Breach response is part of the greater field Incident Management, with the goal to mitigate violations of security policies.

In GDPR, it is the controller and processor that have the operational responsibility to adopt suitable measures for breach response. WP29 has distributed recommendations on four practical steps:

- *"Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk."*
- *"Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organization being informed."*
- *"Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required."*
- *"At the same time, the controller should act to contain and recover the breach." [16]*

## 3.3 Incident management

The National Institute of Standards and Technology, NIST, (explained in Section 3.6.5) addresses incidents in their "Computer security incident handling guide" as:

*“Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.”[17]*

Incident management is the process of handling an incident accurately, covering logging, recording and resolving incidents. Effective incident response management is handled in several steps or phases. SANS Institute has established six steps that have been widely used. NIST agrees to the approach of SANS with the slight change of naming step two detection instead of identification. However, the purpose with these are to respond systematically to incidents:

1. Preparation: Gather and learn the necessary tools, become familiar with your environment.
2. Identification: Detect the incident, determine its scope, and involve the appropriate parties.
3. Containment: Contain the incident to minimize its effect on neighboring IT resources.
4. Eradication: Eliminate compromised artifacts, if necessary, on the path to recovery.
5. Recovery: Restore the system to normal operations, possibly via reinstall or backup.
6. Wrap-up: Document the incidents’ details, retain collected data, and discuss lessons learned. [18]

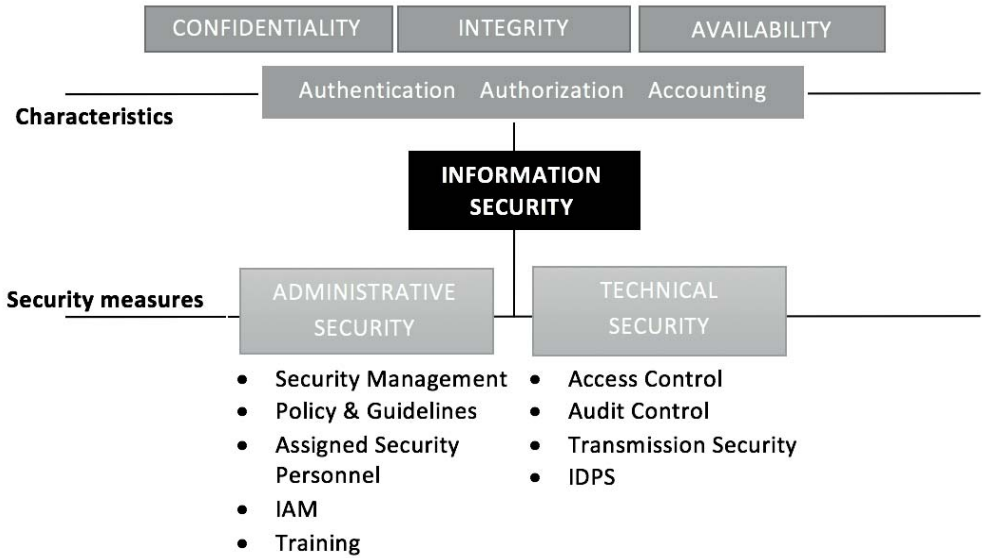
From these 6 steps, the ones that will be covered in this paper are particularly points one, two and three, preparation, identification and containment. These include detection, response, mitigation and reporting, which will have to be altered for compliance with GDPR.

### 3.4 Computer forensics

Computer forensics is part of the greater discipline of forensics, in which various types of evidence are studied to investigate a crime. Computer forensics is essentially the study of digital data, including data recovery and data tracking. The goal is to perform a structured investigation while maintaining a documented chain of evidence of what happened, and obtain the information of why something managed to occur and who to blame responsible. The procedure may be to first physically isolate the device and make a copy of its storage media. Followed by forensic softwares and a variety of techniques to examine the copy [19]. Forensic techniques may be necessary to respond to the requirements of incident reporting in GDPR due to the very specific details that are required to be addressed. The general goal of forensics is to obtain digital evidence to hold someone accountable while keeping the integrity and confidentiality of the evidence. In regards to GDPR, it is not necessary to hold someone accountable but rather to identify what data subjects and objects have been compromised. Further on in this paper the word 'forensics' will be used as 'computer forensics'.

### 3.5 Information security

Information security has for long had the characteristics of the CIA-triad, as seen in Figure 3 below, working for confidentiality, integrity and availability.



*Figure 3 Illustrates the characteristics of information security as CIA and AAA, along with the two categories of security measures*

Confidentiality covers privacy. Integrity covers maintaining the consistency, accuracy and trustworthiness of data. Availability stands for having the data available, even in situations of incidents. [20] CIA often comes together with AAA, Authentication, Authorization and Accounting, which is used to support the CIA concept and can directly be connected to the security measures through the Administrative security and Technical security. GDPR enforces information security on PII through both CIA and AAA. The PII should be accurate and enforce the possibility to update and request a portable extract of collected data. The PII should not be accessible for any other party than the organization which collected the consent. The security measures, from Figure 3, will all be of relevance for compliance with GDPR [21].

### 3.6 Laws, regulations and standards

Incident response is not new in Sweden, but it has not been enforced to this extent until now, covering this broad spectrum of organizations and thorough requirements. However, there are several laws and regulations overlapping with GDPR today. Below follows a few directives and standards for information security.

### 3.6.1 PUL and MSB - Current instance for incident reporting

The regulation GDPR is, in Sweden, replacing Personuppgiftslagen, PUL. PUL was based on the previous European Data Protection Directive, DPD, from 1998. The Swedish Civil Contingency Agency, MSB, is the authority responsible for “issues concerning civil protection, public safety, emergency management and civil defense”[22]. PUL did not enforce general incidents to be reported. However, MSB issues regulations for government authorities in the field of information security. The regulation MSBFS 2016:2 covers it-incident management for government agencies [23]. From 2016, government agencies were forced to report their security incidents to comply with the complementary regulation, KBF (Krisberedskapsförrordningen)2015:1052 and MSBFS 2012:2. In 2016, 214 incidents were reported to MSB. Before the regulation was initiated, MSB handled only about 40-80 incidents a year [24]. Government agencies have to communicate a breach to MSB within 24 hours after an incident has been discovered, including the following parts:

1. Name of concerned government agency
2. A description of the IT-incident including the course of event and measures taken/to be taken.
3. The exact or estimated hour of the incident
4. Hour of incident discovered and if it is still ongoing.
5. What type of incident, loss of information, attack etc.
6. The government agencies’ initial evaluation of the incidents’ magnitude and consequences. [24]

If the government agency has made a police report there is no need to report to MSB.

### 3.6.2 ISO 27000 family

The International Organization for Standardization, ISO, together with the International Electro-technical Commission, IEC, form the specialized system for worldwide standardization. The Swedish Standards Institute ones stated "Standards make the world go around." The family of ISO 27000 standards covers international standards that helps to keep information assets secure[25].

ISO 27001 provides requirements for establishing, implementing, maintaining and continually improving Information and Security Management System, ISMS. An ISMS preserves the confidentiality, integrity and availability, CIA, of information by applying a systematic approach to managing sensitive company information so that it remains secure [26].

### 3.6.3 NIS

The directive on Security of Network and Information Systems, NIS, focuses on achieving a high level of network and information system security across the European Union. It aims to improve cybersecurity capabilities on national level,

increasing cooperation among cybersecurity and EU member states and introducing security measures and incident reporting obligations [1]. NIS will come into effect in May 2018, similar to GDPR. EU member states have until then to make a national interpretation and come up with national laws. The reporting in NIS is to be done to the national Computer Security Incident Response Team, CSIRT, which in Sweden is at MSB. MSB is then responsible to further investigate and announce how this should be done in compliance with NIS. What NIS requires to be reported is slightly different from MSBFS 2016:2. NIS requires the number of users affected, when it occurred and the geographical extent of the incident. NIS only applies to incidents that have a significant impact on the continuity of an important service in the society [27].

### 3.6.4 PCI DSS

Companies accepting payment card transaction from any of Visa Inc, MasterCard, JCB and American Express have to comply with the Payment Card Industry Data Security Standard, PCI DSS.

PCI DSS requires certain documentation to be in order and have recommendations on additional documentation that are not a requirement. First of all, as a recommendation, an inventory of all the assets processing card holder data should exist. This inventory should consist of the following information:

- Cardholder data location
- Cardholder data components (cardholder name, card number, experience date, other sensitive data)
- Data format (clear text, encrypted, masked, truncated)
- Data retention
- Security controls in place to protect the data
- Authorized accounts [5]

Moreover, network diagrams with all connections to cardholder data should be up-to-date, accurate and complete. This would facilitate questions such as how far an attacker may have been able to infiltrate, which cardholder data repositories have been exposed or compromised, if cardholder data was protected (encrypted etc.) at rest and in motion as well as the points of entry to the cardholder environment.

Anti-virus Audit logs should be in place to understand how attackers were able to breach the cardholder data environment. They would be able to answer whether the antivirus detected any malware or not. Together with clues on whether the attackers tried to install spyware, backdoors etc. PCI DSS also recommends having networks logs, OS logs and application logs to be able to understand the extent of the incident. To avoid logs being altered or deleted, logs should be exported from the system where they are generated to a secure server. These should be available for immediate review for at least three months and then be retained for the minimum of one year. Furthermore, keeping the logs at one central place and

for a certain amount of time, it is also necessary to synchronize the clocks of all system components.

Another important part mentioned in PCI DSS is the importance of media inventories. In the event of a lost backup tape, it's critical to have identified the media content to be able to know whether the lost tape contained payment card data or not, if it was readable (not encrypted, hashed etc.), and if so, how many payment cards that has been affected [5]. PCI DSS compliant crypto algorithms and standards are based on the NIST recommendations of AES, TDES, RSA and ECC.

It is important to define the personal data scope and identify where personal data should be protected, whether in transit or at rest. It is as important to keep network diagrams up-to-date and accurate. This since breaches often appears on systems employees know little about, e.g. systems that store data which employees did not know to exist.

Each company may have their own requirements. Visa, American Express and Discovery require to be notified immediately upon confirming a security breach, but for MasterCard the time-span is 24 hours. Further on, Visa requires within three business days from the reported compromise a forensic report to be produced. MasterCard on the other hand requires to obtain the report within 72 hours, no matter if it is business days or not. How many cards of respective brands that have been compromised should be ready to be provided. Moreover, within 10 days, a list of all the compromised cards should be available [5].

PCI DSS requirements mention the need for daily operational procedures and that log reviews for all system components should be performed on a daily basis. There is also a requirement for a formal security awareness program with formal incident response training. The PCI DSS requirements extend beyond those of GDPR but introduces technical aspects and breach notification requirements that may assist to comply with and understand the GDPR.

### 3.6.5 NIST

National Institute of Standards, NIST, is part of the US department of Commerce and have, among others, a division within Computer Security, CSD, and Information Technology Laboratory, ITL. CSD conducts research and development to provide standards and guidelines in areas such as cryptographic Technology and Secure Systems and ITL develops test methods, proof of concept implementations and technical analyses. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. In SP 800-57 Part 3, 'Recommendation for Key Management' (updated Jan 16), recommendations on key algorithms are presented. The approved algorithms for encryption/decryption are the symmetric block cipher algorithms AES (128 bits and higher) and TDA (triple length keys of 56 bits). For asymmetric ciphers we have RSA (2048 bits and higher), for key-establishing along with the Elliptic-Curve-Cryptography, ECC, (256 bits key and higher) for generating digital signatures [28].

## 3.7 Attacks and Intrusions

Identifying the way an incident occurred is one of the key factors for assessing a breach. An understanding of common attacks is therefore of relevance. A breach can be performed in a broad variety of ways, below a few common attacks violating the CIA-triad are listed, either in violation of confidentiality, integrity or availability.

- **Ransomware** usually enters the system through downloading a software program that appears benevolent but carries malicious content. It infects a target machine and encrypts files and PII stored on the system. To retrieve the data, the subject is forced to pay a ransom within a short period of time [29].
- **Phishing** is an attack, typically carried out by email, that aims to fool employees in revealing usernames, passwords and other private information, by acting as a trustworthy entity. Depending on how broad the target group is, this attack may be called spear phishing for a specific target, or whaling if the focus is to tackle senior executives or high-profile targets [29].
- **Network attacks** aim to capture information in motion, such as with the Man-in-the-Middle attack, MITM. This will only be a problem if PII is in transit and there is a lack of strong encryption.
- **Injections** such as SQL, NoSQL, and LDAP-injections has been in the top of OWASP top 10 critical application security risks, for several years and are still the number one security risk in 2017. Injections occur when unsanitized data/scripts are sent as part of a command or query to an interpreter [30]. The data can trick the interpreter into accessing a database without proper authorization and may then extract, e.g., PII.
- **Broken Access control** is this year in place 5 on OWASP top 10. Identity Access Management, IAM, is often not properly enforced. Access shall only be granted if it is relevant for the individuals work. The flaws may be taken advantage of by attackers to access accounts, sensitive files or tamper data [30].
- **Insider access** takes place when employees or IT admins cause harm or fraud through insider access. This may for example be common if separation of duties and the principle of least privilege is not performed, leading to risk of employees taking advantage of their access [5].
- **Social engineering** is a term used for bypassing physical security and tricking/baiting employees into giving an attacker access.
- **Human errors** could be simple mistakes such as mail sent to wrong party but also due to lack of knowledge.

## 3.8 Logs and log storage

This section will explain the importance of logs, present standards, recommendations and different requirements on logging that exists today. Lastly, this section



briefly goes through two types of log storage.

Logs are collections of log entries, each entry consisting of information related to a specific event that has occurred within a system or network. Computer security log management is the response to the greatly increased number, volume, and variety of computer security logs [31]. Typically logs record who took an action, when and where the action was taken and what the action was. One or more logs create an audit trail which may result as evidence, to hold people accountable for their actions [29]. General log-types can be seen below:

- Application logs (e.g, web server, database server)
- Security tool logs (e.g., anti-virus, change detection, firewall, intrusion detection)
- Network traffic, Outbound proxy logs
- User application logs
- Server and workstation operating system logs [32]

Requirement 10 in PCI DSS explains the importance of tracking and monitoring logs as:

*"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs."*[33]

PCI DSS has strict requirements on logging and requires in 10.2 [33] all activities performed by root to be logged. Also, activities on audit trails should be observed, to detect tampering. The possibility to identify changes, additions and deletions can help retrace steps taken by unauthorized personnel. Initialization, stopping, or pausing has to be logged, creation and deletion of system-level objects, invalid logical access attempts and all individual user access to card holder data. They also require at least the following to be recorded for all system components for each log entry and event according to Section 10.3 in PCI DSS:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origin of event
- Identity or name of affected data, system component, or resource

These details provide sufficient information of who, what, where, when and how something occurred. It is critical to be able to link user access to system components accessed, this provides the ability to trace back suspicious activity to a

specific user. Since PCI concerns card holder data, the strict log-requirements is not expected by companies not processing this kind of sensitive data, however, in regards to GDPR it may be relevant.

Several different types of storage exist for storing logs, audit trails and records of digital events. Sequential drives allow you to store much data for a low price. One example of this kind is the magnetic tape drive. Unfortunately, it is slow and lacks flexibility. The tape drive must physically scan through the entire tape until it reaches the desired location to access data stored in the middle. In the early 2017, IBM set a new record for magnetic tape storage, with areal recording density of more than 20 times the areal density used in current state of commercial tape drives [34]. This put the tape drives back in the game competing with the significantly faster Random Access Storages such as hard disks. Hard disks use a movable head system that allows you to move directly to any point on the disk without spinning past all the data stored on previous tracks, which allows for immediate read and write functionality, though costly [29]. It is a trade-off between cost/benefit. Regarding logs, sequential storage may be seen as a uniquely suited storage since extremely large amounts of data can be stored on relatively inexpensive media. But, when it needs to be accessed, it might be too slow to comply with the time-frame of incident reports of GDPR.

### 3.9 Recent incidents

There have been several recent incidents where personal data has been exposed. A few are highlighted in this section to demonstrate the importance of information security and will be used as examples further on in this thesis. Four recent incidents are listed below.

- An example on questionable incident response is the recent data breach of Equifax in September 2017. 143 million peoples personal data got compromised. The notification to the data subjects was not communicated until a month later, which would have been valuable time for the subjects to take subsequent actions.[35]
- The Swedish Transport Agency, Transportstyrelsen, recently had a government information security disaster. In 2015 they handed over an IT maintenance contract to IBM which contained data on the nations safety. The consultants were not security classified due to unclear information classification or ignorance. The data breach exposed members of the military's most secretive units, police suspects, along with PII of the citizens of Sweden.
- NotPetya and BadRabbit are two ransomware attacks that spread during the summer and autumn of 2017. They appear to be from the same source and encrypt the content of computers and require a ransom for it to be returned. The ransoms caused serious disruption and chaos at large firms in both Europe and in the U.S., including hospitals, shipping and transport firms, supermarkets and hotels [36].
- Ashley Madison, a Canadian dating site for married couples wanting to have an affair, had a data breach in 2015. 37 million user accounts were leaked,

leading to tragic ends for many couples [37].

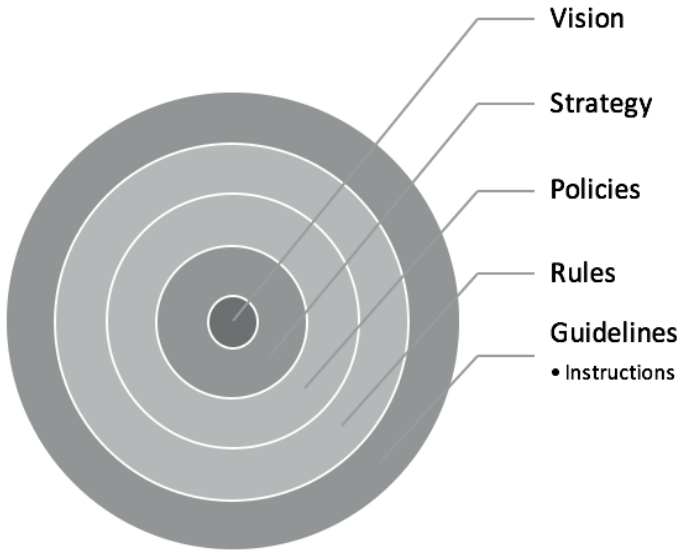
This chapter will present the empirics consisting of 11 interviews conducted at the consultant firm Knowit, together with an additional deeper interview at a fintech company, as well as a conducted forensic investigation. The main objective has been to get an understanding of how companies today are working with information security and current approaches to breach response.

## 4.1 Interviews

As presented in Section 2.4.1, the interviewed consultants were security and legal consultants from Knowit, with many years of experience in the field. The goal was to get an understanding of the current situation in the field, as well as discuss their approach to the problem statement together with their understanding of GDPR. In sum, the interviews expressed a general lack of proper incident management at organizations. The obtained reason for this was general lack of awareness of consequences, as a result of a non-existing vision for information security, see Figure 4.

The interviewed consultants had a wide background of experience such as, setting up the first CIRT in Sweden, previous positions at Datainspektionen, GDPR specialists, Incident Management Consultants and forensic analysts. This broad spectrum of insights contributed well to the understanding of how companies handle security issues today. The consultants areas of expertise, their experience with breach response and their views on the problem statement were examined. Many of the interviewed employees had performed incident-response controls at client sites which brought concrete examples of common shortages.

Figure 4 illustrates how lack of vision leads to malfunction at the other levels, in accordance with the interviews. The interviews brought forth the common state of no appointed strategies, no policies, no rules, no guidelines nor instructions for employees to adopt on how to proceed. Without guidelines, employees do not know how to act if an incident occurs.



*Figure 4 Illustrates different layers where information security should be assessed, with vision in the core.*

The obtained understanding of common security shortages are:

- No one responsible for information security incidents
- No information on security goals or visions
- General lack of knowledge about information security
- Lack of steering documents
- If steering document exist, it is not followed
- If logs exists, they are not being monitored
- No information classification procedure
- No accurate Identity Access Management
- Employees do not know where/how to report
- Governments are not as well prepared as one could expect from previous requirements
- Incident response requirements differ too much between companies, a general straightforward procedure to follow does therefore not exist.

Positive insights:

- Companies being PCI DSS compliant have a good foundation
- Common with an in advanced established contact for forensic investigation

To summarize, engagement from top management in security related questions is a shortcoming. This has resulted in a general lack of awareness of information security and its risks throughout organizations. It is common to put all trust in a forensic analyst when an incident occurs. This understanding has shaped this thesis in highlighting the focus on getting procedures in place, since a forensic analyst can not make an investigation if, e.g., there are no logs to analyze.

## 4.2 Observations at fintech company

Two sessions were set up at a fintech company, with their CISO. Together with a security consultant from Knowit, existing incident response procedures were investigated along with recommendations on improvements. Appendix E covers a number of questions discussed. The questions ranged from current security measures to future plans.

The fintech company had to comply with both PCI DSS and GDPR, which made it an interesting company to meet. One security measure was the Disaster recovery plan, DRP, that each system owner had to read and fill out. The DRP contained an inventory of what assets and PII that were stored, as the recommendation by PCI DSS in Chapter 3 section 3.7.4. The focus of the plan was to prepare the company for production disruption. Contacts to relevant people were written down for each system together with system descriptions, network interfaces, critical files keys, etc. The company also had a Business Continuity Plan to support management in case of a disaster.

Regarding the question *if they will be able to extract the relevant data to report when an incident occurs*, the company put their trust into the forensic analyst. The company itself did not have the competence in-house. When an incident occurs, they would call a forensic analyst for the investigation. The company itself focused on two things. First, to set up an incident response team fast. Second, grant the forensic analysts access to systems and centralized log archives along with making information available with contact details to relevant employees, etc.

Having established security policies are the first step towards a well-performed incident response. During the second session, elaboration on their incident response plan was done. It included steps to set up initial communication tools, involve the right people and actions to take, such as maximizing logging on all units, increasing log monitoring, disconnecting from network, limiting firewall rules to mitigate incidents, replacing crypto keys and finally conduct a report.

By looking at the observations made at the company, a well-functioning security procedure was in place since they already were compliant with PCI DSS.

## 4.3 Forensic investigation

The aim of the forensic investigation was to get a better understanding of the forensic procedures and the struggles a forensic analyst faces. The investigated case was about identifying what had happened and why. The entity of investigation was a hard-drive from a kiosk-window-terminal. Using a write-blocker, a dd-image of the hard-drive was taken to be able to analyze without risking altering the real

disk. The hash algorithm MD5 was used to calculate a checksum to make sure no changes had been done to the drive following the closing of the disk. Relevant logs got extracted, such as event-logs, chrome-logs and file-system-logs. From these logs, a time-line was created and the search for suspicious actions initiated. A final hypotheses of what had happened managed to be brought forth and a report was written.

If no personal data is stored, there is no incitement for personal data crime/breach. Only if data is relevant to an organization's business should it be stored, kept and protected. This chapter presents the result of the theoretical literature study together with the empiric interviews. The chapter is divided into three sections corresponding to the three subareas earlier presented as:

1. Clarification of the regulation - What needs to be reported and to whom.
2. Forensic investigation - How to obtain the requested information to be reported. E.g., how can we narrow down the scope of a breach to not assume all subjects in a database have been leaked.
3. Incident management - Investigate methods and processes in order to provide best possible environment for forensic analyses.

## 5.1 Clarification of GDPR

This section presents the result from mainly the theoretical study. The GDPR has been thoroughly examined together with observed standards presented in the theory, NIST, ISO, etc. From these sources the below understanding has been obtained, presented in three parts:

- Article 33
- When PII can be considered not to be at risk
- When PII might be at risk and what actions then to take.

### 5.1.1 Article 33

Previously, it used to be enough just acknowledging that a breach had taken place without any tangible legal requirements for further actions. Moreover, no further investigations were done due to this being very time-consuming and costly. Now with the GDPR approaching, procedures for further action needs to be established and recognized. The main concern for companies today is how to properly understand the regulation and how to make the adequate adoptions. Misleading headlines and media information are circulating on sanctions and time-triggers. However, there are several paragraphs in GDPR which are open for self-interpretation.



However, mis-interpretations should not be confused as such. What might cause these misunderstandings is the fact that a requirement in an article of GDPR often comes with exceptions. These exceptions are not always presented directly after the requirement itself, enabling for misunderstandings and unjustified conclusions.

In case of a breach, the supervisory authority to report to in Sweden is Datainspektionen. The four parts of what to report are described in Article 33. These parts are:

1. *The nature of the personal data breach, including where possible, the categories and an approximate number of data subjects concerned together with the categories and approximate number of personal data records concerned.*
2. *The name and contact details of the data protection officer or other contact point where more information can be obtained.*
3. *The likely consequences of the personal data breach.*
4. *The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[10]*

Point one raises most concern and will be one of the main focus areas in this report. The approximate number of personal data records together with the number of data subjects will be analyzed.

Note that the report only has to be conducted unless *the personal data breach is unlikely to result in a risk to the rights and freedoms of a natural person*. To be able to state whether this is the case or not, the category of the data concerned, is of interest. If the breach is likely to result in economic or social disadvantages for the data subject or result in discrimination, identity theft or fraud, then there is a risk to the rights and freedoms of a natural person. The fact that GDPR restricts organizations from storing information they do not have a valid reason to keep is a good reason for companies to finally get rid of unnecessary data and save storage-space. To conduct an asset check as PCI DSS recommends and go through all collected information is a relevant step in order to be aware of what data is being stored where. It is also a great way to discover data that is not as protected as it should. Drawing on what was mentioned in the theory, most breaches take place on systems where data weren't known to be stored, this is one of the things GDPR addresses and aims to reduce.

### 5.1.2 No subject at risk

When an incident occurs, the degree of the incident in terms of whether PII is at risk, high risk, immediate risk or at no risk, needs to be determined. To be able to prove the latter, not at risk, the exposed data has to be *unintelligible*. GDPR gives encryption as an example to obtain this state but provides no further details. By looking at PCI DSS, the NIST recommendations are followed and the encryption is only approved if it is aligned with the recommendations of NIST. Today this would be AES or TDES. For key management and signatures, RSA and ECC would be valid. These are referred to as the state of the art algorithms by NIST. A reasonable approach to adapt for GDPR would be to follow these

recommendations of NIST. The exposed PII would then not be considered to be at risk, as long as the key is certain not to have been compromised. A subsequent question that previously has been discussed by many parties is whether a breach of unintelligible data still needs to be reported to concerned authority. Working Party 29, WP29, published an opinion in 2014 where they argued for that a breach still should be considered a breach even though the data was encrypted with state of the art algorithms [38]. However, in October 2017 they published a paper on 'Data breach notification' in regards to GDPR, concluding the contrary [16] :

*"If personal data have been made essentially unintelligible to unauthorized parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms".*

Opposed to their previous statements, this is currently the latest analyze on the subject. However, they add that circumstances could change and notification be required later on:

*"It should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required."*

Moreover, an alternative to encryption would be to prove *unintelligible* through other means. If we could, through for example information classification and proper IAM, be able to conclude that the intruder would have managed to gain an access with a certain level of authority and would with that authority only be able to view data with classification "public". This would be considered a breach unlikely to result in a risk to the rights and freedoms of natural persons. This step is important and will be further discussed in sections 5.3 and 5.4, including assessment of what measures that need to be set up on both a physical and structural level to be able to reach the above conclusion.

This section has explained two paths reaching the conclusion of subjects not being at risk and no further actions required. These have been (1) if the exposed data was encrypted with state of the art algorithms and (2) demonstrated other means of unintelligibly, illustrated in Figure 5.

### 5.1.3 Subject at risk

If the initial hypothesis did not reach a path leading to a *subject not at risk*, the incident should be considered as *personal data might be at risk* and the procedure should be followed from there. A forensic investigation would then be necessary to be able to further specify the degree of the incident and state whether the situation is a risk, high risk or immediate risk, in accordance with Figure 5. Figure 5 is a clarification of what time-spans and procedures that GDPR enforces depending on

the *severity of risk*. The definitions of the different degrees of risk are not clearly defined in GDPR and await further clarification.

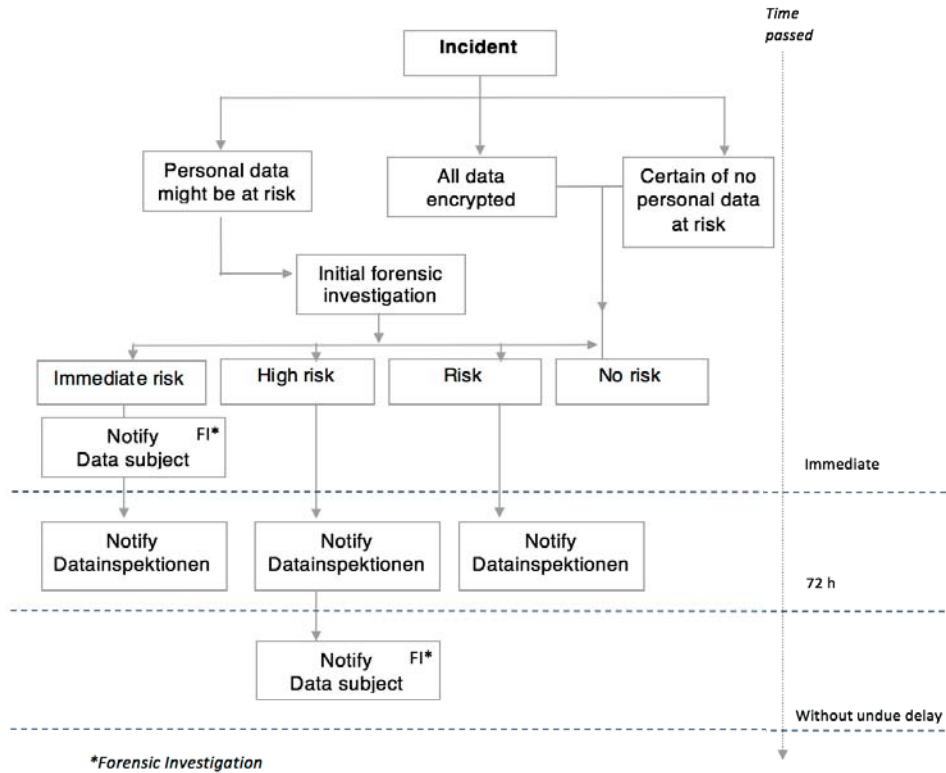


Figure 5 Actions regarding risk to PII. Illustrates the severity level of an incident and actions to take depending on the level of risk to subjects' rights and freedoms.

An initial approach to assess the degree of risk is to examine the DPIA where the risk already has been assessed prior to carrying out the processing operation. The DPIA is assumed to be written in a more generalized manner and therefore may not be applicable to the specific circumstances of an actual breach. However, the DPIA would point in the right direction for further investigation as a good starting point. If the risk would be considered 'immediate risk' to the rights and freedoms of concerned subject, such as for sensitive PII, the data subject has to be notified immediately and the supervisory authority, Datainspektionen, as the second point to alert. If it instead would be a 'high risk', the notification to Datainspektionen comes first and the second point to alert would, in this scenario, be the data subject. Note that the data subject does not need to be notified within 72 hours in this case, but without undue delay as stated in recital 86, see Appendix D. If the effort to notify all subjects would *involve disproportionate effort*, a public communication that informs the affected data subject in similar effective manner would be feasible. A disproportionate effort could be when the PII does not contain contact details. It then might exist a possible way to obtain the details, but no clear procedure of actions. GDPR would then accept the breach to just being

announced on, e.g., their web page. If the risk would be categorized as only 'risk', the data subject does not need to be notified at all, only Datainspektionen. GDPR recognizes that 72 hours is a short amount of time and is aware of the risk that it might not be possible to hand in required and necessary information in time, paragraph four in Article 33 responds to this as:

*“Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay”. [10]*

Accordingly, GDPR allows for further notifications in phases. This is likely the situation for complex breaches with conducted forensic investigations for establishing the nature of the breach and extent of compromised PII. Many parts of GDPR turn out not as strict as they first appeared. After all, GDPR is not here to make companies pay sanctions but rather to create awareness on information security and protect the rights of the individuals. However, where GDPR might be a heavier burden than previously expected is within the forensic investigation. To be precise, obtaining the following information:

- The approximate number of data subjects
- The approximate number of data records
- The exact subjects affected

To conclude, the process-scheme in Figure 5 has been developed through discussions and interpretations. It is a clear guidance of what needs to be done within what time-span depending on severity of risk.

## 5.2 Forensic investigation

Incident forensics may be the first step of a response strategy with logs among the richest source of evidence. This section will start to identify how the role of the forensic analyst will change, followed by an approach for initial hypotheses of breached data, finalizing with recommendations on log management. All aiming to narrow down the suspected amount of data loss and to obtain the summarized factors from the previous section, the number of data subjects, numbers of data records and exactly what subjects.

### 5.2.1 The forensic alteration

What previously mainly appeared in major investigations of crime or the like, now might be necessary for any general data breach. The work of a forensic analyst will not only be conducted for evidence in court but also for identifying the severity level of risk to a subjects' rights and freedoms. The investigation is recommended to be performed by accredited individuals to have it properly performed. The actual forensic work might not change, only its importance and load. It is possible the work will actually be easier. This since GDPR requires certain procedures to be in place which will facilitate an investigation, such as relevant logs being stored and preserved in an optimal manner.

## 5.2.2 Intrusion points

The chosen approach, to obtain the requested information to report, has been to focus on the intrusion points. To find out what to act upon and what logs that are of interest, the possible ways of getting into the system have to be identified. Each unique entry point may need a unique setup for containing a breach. However, some identified intrusion ways, based on attacks previously mentioned, has here been categorized into three groups. These are:

- Compromised authentication
- Malicious code
- Capture of data in motion

A compromised entry point would be any kind of unauthorized access to a system. These three has been chosen since the attacks included in each category may use similar approaches for identifying the compromised data.

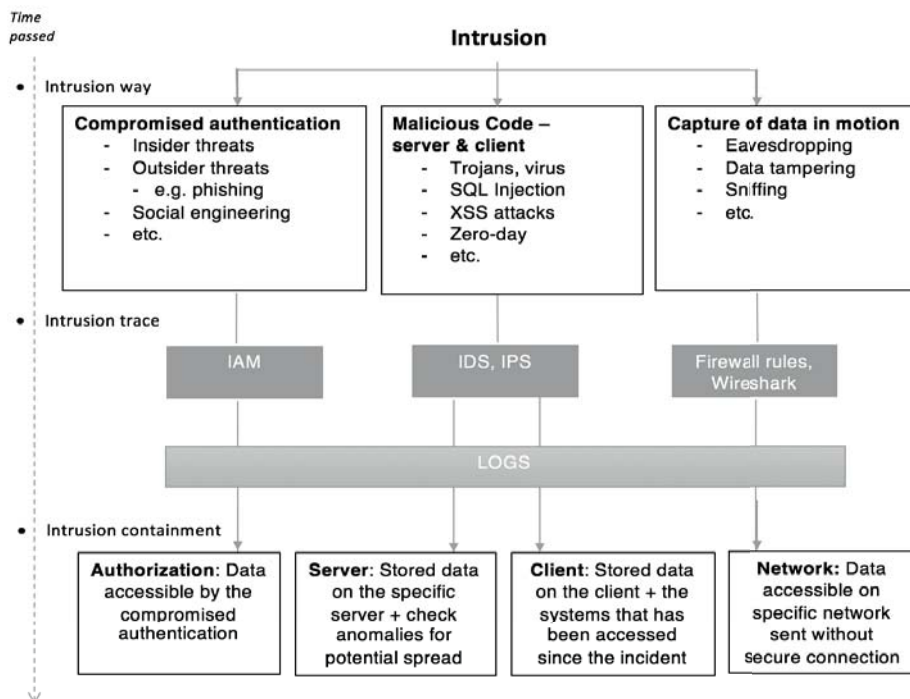


Figure 6 An initial approach to forensic investigation that groups different types of threats into groups based on their intrusion point. Each group could then use similar measures of containment.

The first category covers *compromised authentication* which is the goal of any kind of attack against credentials or access rights, illustrated in the left path of Figure 6. Among the attacks previously discussed in Section 3.7 that are covered in this category, are phishing, social engineering and insider threats. Basically, anything

that would give direct access to data at rest through obtaining someone's access. The common factor is that the intruder (insider or outsider) is authorized/falsefully-authorized and granted a certain set of authorization depending on what kind of IAM that is in use. This authorization is what will contain the compromise to not suspect all data to be exposed. Some common IAMs are Rule-based access management, Role-based access management, Mandatory access management and Discretionary access management. No matter what IAM that is in use, an Access List, Access matrix or similar should be in place that would be able to identify a certain user/employees authorities. To give an example, let's say we have identified, through proprietary data filtering, that the user Alice has been leaking secret data. Whether it truly is Alice or if it is someone that falsely has been authenticated as Alice we do not know. But what we do know is that all data Alice is able to access should be considered as potentially compromised data. If role-based access management is being used we could look at what data-files the role of Alice is granted, files that are classified as public, confidential and secret, or even top secret. The classification of data is here crucial. Without a proper data classification, it would not be possible to categorize the data and therefore neither be possible to manage a proper IAM. To limit the impact, the principle of least privileged should always be in use. This means giving employees the least possible authorities to perform their duties. If on the other hand, the admin account would have been compromised through, e.g., an escalation of privilege attack, unfortunately, all data in the system could need to be seen as leaked.

The second intrusion point has been categorized into covering attacks injecting malicious code to a system. This category covers a broad range of different types of attacks such as SQL injections, XSS, buffer overflow, backdoors, virus, trojans and much more. The category could be sub-divided into the client resp. server-side since the procedure of containing a breach slightly differ. For servers, the breach may be isolated to the data stored or processed on that specific server. To make sure the malicious code hasn't spread, a look at the firewall logs may be of value. If the system, e.g., only used to get input data but now also carries out output data, there is a risk of the malicious code spreading to other systems. Checking for abnormalities would spot this change and likely trace the code to a new location, in which might have been compromised, the Active Directory, AD, in worst case. Moreover, on the client side, first of all checking what data that is stored on the client. Secondly, find out to what systems the client has access to. By looking at the firewall logs, trace of what systems the client has accessed from the time of the breach, and from there on containing the breach to data in those systems.

Data in motion transmitted over a network can be captured through, e.g., data network eavesdropping, data tampering or data theft. This is the third category of intrusion points. The first action to take is to identify what network that has been compromised, such as an external guest network or internal, with files and catalogs accessible. Next step would be to identify what systems communicate over that specific network. Looking at the firewall rules we may see what systems that the network may communicate with, e.g. Sharepoint and through what ports. Ports such as 443 with https traffic would not be at the same risk as un-encrypted traffic through FTP port 21 or http on port 80. All servers that has been accessed through those may need to be assumed compromised. On the other hand, if the

data was sent encrypted, that would be enough of a safeguard to no longer assume that risk. Wireshark could here be a good tool to use for observing network traffic.

The three intrusion points that have been examined have demonstrated an initial way to state what data that has been compromised. Until a forensic investigation has been performed, just by looking at these attack-paths, it will be possible to narrow down the scope of subjects being concerned to at least a little less. This will be necessary if no forensic analyst will be able to obtain the information needed in just 72 hours.

### 5.2.3 Logs and log storage

The fundamental problems with log management are the high number of log sources and generation of large volume of log data that not only need to be stored but also monitored. Log management is essential to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Logs are the core of any forensic data investigation. All attacks discussed in previous section results in the need to rely on proper log management to be able to obtain the requested evidence of an incident. Too selective log management results in no evidence. Too much logs leads to very time-consuming investigations and difficulties in finding the logs of relevance. GDPR has not yet given any recommendations nor guidance on what to log. In this section, recommendations have been made from looking at other laws and regulations mentioned in the theory.

Log-decisions generally will depend on what PII that exist in a system and none the less, where it is located. After identifying the PII and sensitive data, the focus should be put on sufficient logging for all access to these systems/servers. Some fundamentals in logging can be summarized as the following:

- Make sure the time-stamp is accurate and synced to a common time source
- Make sure the logs tell you *who* did *what*
- Keep the logs read-only to avoid tampering
- Don't keep sensitive information in the logs
- Do not store useless logs
- Do not log data unless it is legally sanctioned
- Centralize logs

Logs not to be stored would be sensitive personal data and logs that would be of no help in an investigation. Following the advice of PCI DSS, each log entry should be composed of type of event, date and time, success or failure indication, origin of the event, affected data and a user identification. A user identification should be able to track a user's action to one specific individual which results in shared accounts being unacceptable. Account Management actions are also of importance to be logged to be able to see what users that have existed, viewed, created, updated and deleted.

The next concern to raise is the retention period for logs. If any legal requirements apply for the retention those should be prioritized, such as for card data

with PCI DSS. As with GDPR, nothing is stated, and logs should therefore only be retained for as long as necessary. Since it usually takes months to discover a breach the optimal retention period is hard to define. PCI DSS has made the requirement to retain logs for one year and the last three months must be easily accessible. This is a good feasible approach to adopt in the case of GDPR for systems storing sensitive PII. Systems with regular PII might argue that one-year retention policy would constitute to disproportionate effort which is justified if the PII would not risk the rights nor freedoms of the subject.

Long-term storage is not meant to be accessible unless an investigation is being performed. Drawing on the theory in Chapter 3, mechanical disks is a suitable option regardless of its limitations of being very slow. Whereas the 3-months storage needs to be accessible and easy searchable which works for centralized log systems on hard disks. Every year more and more logs will be available to extract, and even with a retention period of only 3 month the storage will end up expensive and the dilemma of cost-benefit is confronted. An alternative is to use cloud-based services, such as SPLUNK. It exist several of different cloud-based solutions, but whether to use a cloud-based or a distinct offline solution is a discussion not taken in this report. Whatever storage is chosen, all activities on the storage system need to be tracked to identify abnormalities and also preferable having calculated hashes for all data sets stored to spot changes.

To establish and maintain a successful log management, an organization should develop standard procedures and guidelines for performing log management. This is part of the greater field of incident management that will be examined in the next section.

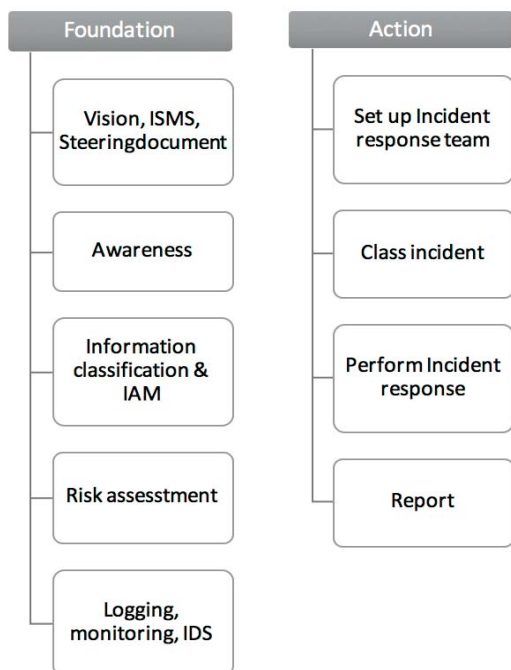
## 5.3 Incident management

As incidents no longer is a question of if, but rather when, procedures of how to respond needs to be defined and adopted. From the empirics, it was clear that this is where most companies today are lacking. ISO 27001, NIST, SANS and others have settled guidance and standards of how to perform proper incident management. This section will stress some important points relevant to the GDPR.

An initial vision of where the company is aiming is essential, as illustrated in Figure 4 in Chapter 4. Top management needs to address the organizations vision in information security and demonstrate through steering documents and policies how this should be enforced. There needs to be a strategy in place, policies established, rules to follow and guidelines of how to do so. Not until then will it be possible for each and every employee to have a chance to act accurately upon an incident. A good step forward would be to establish an Information Security Management System, ISMS, in Sweden called LIS (Ledningsystem för Informationssäkerhet). ISO 27001 is a specification on creating an ISMS as part of an organization's general management systems. ISMS is a set of policies and procedures for systematically addressing and managing an organization's sensitive information. The goal is to limit the impact of a breach by minimizing risks and ensure business continuity. This consist of identifying system owners, processes and action plans for incidents. Support documents for this exist at [www.informationssakerhet.se](http://www.informationssakerhet.se) in



which well explains these procedures.



*Figure 7 Illustrates two levels of security measures categorizing Foundation as procedures that should be in place and Action as actions to take when the incident occurs.*

Looking at Figure 7, a well-functional incident management consists of the two parts, the in advance established foundation and the actions to take once the incident has occurred. As important as having guidelines to follow, each and every employee has to be aware of it. Awareness is crucial and it shall be managements responsibility to make the security guidelines reach out to the employees. Trainings are a great tool to get employees evolve in security questions. Awareness could also cover the organization's awareness of potential risks. Risk assessments are the tool for this. The GDPR requires data controllers to conduct Data Privacy Impact Assessments, DPIA, where privacy breach risks are high, to minimize risks to data subjects. DPIA is a type of Risk assessment but focuses only on PII and not the overall risks for the company.

Moreover, what needs to be in order prior to an incident is information classification. In order to be able to prioritize and calculate on risks, the processed information needs to be labeled. Common sensitivity classifications for commercial use are public, sensitive, private and confidential. Each category may then have different requirements for processing data, e.g. degree of encryption. Especially within GDPR this will be of high value in order to quickly be able to state

whether the exposed data might risk a subjects' rights and freedoms. Information classification also enables the use of Data Loss Prevention systems to prevent sensitive-labeled data leaving the organization.

IAM is also part of the technical security that needs to be properly set up. For best use, it is important to follow the 'need-to-know-principle' and the 'principal of least privilege' in order to grant employees the lowest level of access possible. This will especially be of importance considering the first intrusion point mentioned in the previous section, compromised authentication, to minimize the access for possible intruders.

Log management is the final crucial foundation that needs to be in place prior to an incident. An organization should define logging requirements and then develop policies that clearly define mandatory requirements and suggested recommendations for log management activities, including log generation, transmission, storage, and analysis. It lays in the hands of the organization's management to provide necessary support to develop these processes. The operational processes of log management should include monitoring and detection. Anomalies should be detected and investigated. IDS softwares exist for this cause and should be used.

This foundation is not a very common engagement at organizations today. However, its importance is getting more and more attention, thanks to recent incidents that likely could have been avoided with the right support from top management. Some companies entirely rely on an external forensic analyst when incidents occur, and take no actions however before nor after. Even if a forensic analyst will be called in whether there is a process for it or not, the breach will most likely be much better contained if there is one. The preparations are done not only to give the forensic investigator the best feasible starting-point to perform an investigation but also to be able to handle the entire procedure that an incident puts one in, from identifying the incident in time to know who to call and communicate with.

The right part of Figure 7 address suitable measures to be taken upon a breach. GDPR enforce information concerning all security-related events to be directed towards the controller. It is the controller's obligation to gather the incident response team, and forensic analyst if necessary. The controller shall classify the incident based on risks to individuals, involving relevant sections of the organization. Depending on the degree of severity, notification to the supervisory authority and, if necessary, to affected individuals are performed. The controller triggers the incident response plan working for containment and recovery. An entire Incident management plan is more complex than this, but in regards to GDPR, the steps mentioned above is the ones that should be in focus to be able to identify and contain a breach.



This chapter will discuss some aspects of breach notification within GDPR based on the result.

## 6.1 Engagement from top-management

Whether top management sees their engagement in security-related topics as justified may be a concern. GDPR is just one among many legal frameworks companies need to comply with. But as GDPR has gotten significant attention in media, the common public has become aware of it and realized the value for themselves of choosing companies well-compliant with the regulation. In addition to being a legal framework to comply with, GDPR has raised the awareness and thereby the acceptance of breach tolerance. Being the victim of a breach could result in a devastating loss. If a breach is not handled properly by a company, it may face customer's and client's loss of trust and transfers to competitors. On top of this reputational loss, the grand sanctions apply.

As full compliance with the regulation by May 2018 will be rare, companies having the muscles to race and shine at the head of compliance have made a tactical business move. Credibility will be demonstrated not only through audit, but from the public's choice of decisions. Concluding, when GDPR becomes a question of competition, top-management may actually see the value and engage.

## 6.2 How private is private data?

PII is the core of GDPR. Since notification to Datainspektionen only has to be communicated if the exposed PII would conflict a person's rights and freedoms, one thing that would be relevant to look further into is the value of PII. What information would actually conflict a person's rights and freedoms and how the severity of risk is assessed? We use social media to go public with things we do, things we have done, our thoughts and habits. If this same information were to be provided from another source than ourselves, would my rights then be violated? If we were to map all public data that we have posted, with what is categorized as being private data, there sure would be plenty of correlations. Someone may share their religion on their facebook-profile. But as religion is being categorized as sensitive PII, companies have to do everything they possibly can to protect this

information. The effort may be seen as disproportionate. However, where we face the problem, companies do not know whether the subject would not mind sharing their religion in public or not, which ends up in the need to treat all subjects the same.

In the case with the Ashley Madison breach, where all their members having an affair were leaked, the PII itself was not what worried people but the association of the PII and the site. Simply the fact that they were members of the site. If a grocery store's member database would leak, the consequences would not be nearly as bad. This complicates general guidance on what PII that cause what degree of risk. It will always depend on the situation, which supports Datainspektionens approach to make an assessment in each individual case. Aggregation is another aspect adding complications. The exposed information solely in its current context might not be of risk, but if this data would be possible to connect to other data of no risk, sensitive information could appear. Suppose the only PII Ashley Madison would store would be an email address, if this email would not directly be associable to a person due to its meaningless name, the subject might feel safe. But what if the grocery store stored both email and name. That name would then be possible to connect with Ashley Madison. This demonstrates the need for treating all data collections with much care and always assuming the worst.

## 6.3 The impact of GDPR

The GDPR has been criticized heavily, some say it is impossible to be compliant while other talk about it as "if it happens", hoping it will never come into effect. Many interpretations have also been made. Media like to amplify the critical parts but, not often the full picture. The new rules are certainly stricter and more demanding for organizations than current rules. However, some rules that seem new already exist today and most of the requirements of GDPR have exceptions with notably easier obligations which, as long as attempts of effort can be demonstrated, instead may be adopted.

### 6.3.1 Reporting

The initial details to report only cover an approximation of what subjects and objects that are concerned, which could be possible to obtain through the approach of point-of-intrusion in the second part of the result. However, when it comes to notifying concerned individuals it is getting more complex. There will always be a trade-off on what and when to report. Historically, organizations have been very reluctant to reveal their breaches since it would result in loss of trust and customer confidence. Today with sanctions applied, reporting is even less in favor to an organization. Organizations may resemble this to raising their hand on the highway announcing that they are driving too fast and would like to have a speeding-ticket. Some may argue that, the less detected the better, fostering weak detection systems and less being reported. However, absence of evidence is not evidence of absence. If not reported, the sanctions will be even higher and subjects might be at risks. Since breaches are becoming unavoidable and information that

is kept might actually cause damage and personally detrimental impact if leaked. It is necessary to detect the breach before the entire business is put in danger.

### 6.3.2 Data erasure

The requirement of the possibility for subjects to request to be erased, may be seen as a problem for incident management. Will subjects, for example, need to be deleted in backups and logs as well? There is today no certain rule for this, just thoughts and guesses can be applied. As PII is not supposed to be stored in logs, this should not be a problem. If PII, however, is stored in logs and a subject would request to be deleted, this would lead to logs being changed and altered. This would result in the logs not being valid as evidence any longer since it has been changed. This would therefore not be a reasonable solution. To remove a subject from a database backup would not be worse than some extra efforts, but if the person would need to be erased from not only structured data such as databases but also from unstructured data, it would add complexity. GDPR has not yet made any exception for unstructured data. Additionally, some information is not allowed to be erased due to other laws or regulations that weigh heavier, leading to the next hurdle, to keep track of what is ok to delete and what is not. The degree of erasure can also be discussed, since a deleted file is not really gone. Is it enough to just remove the pointer to an object, as when deleting a file, even if it might be obtainable through an investigation. Will it need to be overwritten, cleared or even purged? Since this seems as disproportionate amount of effort to attempt on specific records, in the case of a subject requesting to be deleted, it is not a very likely approach.

### 6.3.3 Time aspects

Several parts of the regulation raise questions on how the articles should be interpreted. Article 33 state that "Without undue delay" no later than 72 hours after "having become aware" of the incident one shall notify the breach to supervisory authority [10]. First of all, how long time is undue delay? Secondly, when does the timer start on "having become aware", is it when someone first raises the question of that something might be wrong, or when the controller gets the final message that a breach has taken place. WP29 considers that a "controller should be regarded as having become aware when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised" [16]. Which does make sense but still enables room for discussion. In some cases, it will be clear that a breach has taken place whereas in other, the emphasis should rather be on the action of investigating whether it is, a personal data breach or just a breach.

## 6.4 Breaches

A breach can be ugly and if not prepared for, unfounded demands and internal accusations to IT staff may emerge. Breach responses have for long been the responsibility of IT. Now, when breaches daily are being seen in newspapers, and

privacy is becoming a demand from the public, trust and reputation easily get infiltrated by breaches. A well-managed breach response could save a company from losing both their customers trust and money.

The process of breach response requires combined efforts of IT, legal, communications, operations, and PR, and all need to keep good communication to act uniformly to mitigate rumors and negative reactionary behaviors. GDPR announces the obligation on the processor to alert its controller of potential breaches. The controller has the obligation to act on any alert, justified or not, to determine whether a breach has occurred. Since these roles are new for some organizations, extra enforcement needs to be on integrating these in existing processes and documents. It is then up to the controller to assess whether the breach triggers a breach response plan and needs to be escalated.

The incident response will need both the technical and administrative security measures to be in place. The processor and controller need both accurate preparations and a plan of immediate actions. People, technology as well as processes need to be improved and adapted. Awareness throughout the company to report upward, is an essential element to detect and address a breach and shall not solely be left to the processor.

Based on obtained results and analysis, this chapter presents the conclusion of the problem statement *How forensic methods and preventive measures must be adapted to handle the new requirements of breach response in GDPR*. The conclusion is divided into three subareas that were found to be relevant for identified challenges. These are (1) Clarification and an accurate understanding of GDPR, (2) Obligations of the forensic investigation, and (3) Incident management.

1. *Clarification of the regulation - What needs to be reported, when and to whom:* The regulation is not as strict as media normally describes it, at least not in regards to breach notification. The foundation of compliance in breach response consist of having a clear understanding of the regulation articulated, what and when to report. Whether notification shall be done to Datainspektionen or also to affected individuals. Figure 5 in Section 5.1.3, a scheme of the process of reporting illustrates the measures to take depending on what PII that might be at risk and its severity. Exposed Sensitive PII would lead to controller's immediate report to concerned individuals and thereafter to Datainspektionen, all within 72 hours. However, if the condition of 72 hours is not possible to meet and a valid reason and effort can be demonstrated, GDPR allows for notification in phases. Moreover, if the PII not would be sensitive PII, the opposite order of reporting should be performed, starting with Datainspektionen followed by the subjects. Only incidents that might risk an individuals rights and freedoms have to be notified, e.g. *state of the art encryption* alleviate this risk regardless of data concerned. The trigger points and an understanding of how to accurately classify an incident in order to take appropriate measures are of relevance.
2. *Forensic investigation - How to obtain the requested information to be reported. E.g. how can we narrow down the scope of a breach to not assume all subjects in a database have been leaked:* To obtain the requested information to report, and narrow down the scope of a breach to not assume all subjects in a database have been leaked, a relevant measure is to quickly involve the controller and competent people. The initial decision can then be made, if a further investigation is necessary or if it is possible to state that the potentially exposed data is not at risk.

It is not an easy task to quantify what subjects and objects that have been compromised. What GDPR requires compared to previous regulation is



simply that this assessment has to be done. The approach taken in this thesis was to identify the intrusion point and from there make an initial hypothesis of the scope of the breach, as described in Figure 6 in Section 5.2.2. Whether the intrusion point is a compromised authentication, malicious code or data in motion, different measures exist to contain and limit the scope of the breach, using log management as the fundamental tool. This approach could be of interest for making the initial decision of the severity of the risk and also as a tool when the time is too short for a complete and thorough investigation.

3. *Incident management - Investigate methods and processes in order to provide best possible environment for forensic analyses:* To facilitate a potential investigation there are recommended procedures within incident management that should be followed. As concluded from the result, the primary step to take in order to enable compliance with GDPR is to have a clear vision concerning information security and incident management. This will be necessary to properly manage the needed and required procedures in GDPR. Vision and security strategy should come from top management rather than from the IT department to effectively be integrated throughout the company. Whether the incident response is handled in-house or by an outside specialist, there should be a clear process of what to do and who to involve, processor, controller, specialists, etc.

Best possible environment for forensic analyses consists of an established contact that quickly will be able to grant the analyst access to relevant log systems and provide further contacts. Clear roles and responsibilities are crucial. An updated asset inventory is of value to determine what data files are on what systems and a search-able log environment containing sufficient logs. This should enable a great starting point for the analyst to define exposed data and state the severity of risk.

To conclude, GDPR is implemented by resolutions primarily to reinforce individuals' rights of their own data, and not to find flaws and issue sanctions. Breach response in compliance with GDPR consists of having a clear understanding of what and when to report as well as having an initial approach to obtaining the exact number of affected individuals. Finally, to have a vision and strategy from the top of the company so that resources, the right people and a budget, can enable procedures for an investigation. Essential preventive measures that need to be in place to be GDPR compliant are primarily awareness and a response plan. Management, security professionals as well as employees need to be aware of common attack methods, they need to be aware of what PII they are processing, and what degree of data confidential classification they have in their applications. This is of relevance in order to take proactive steps, recognizing intrusions when they occur and respond accordingly. To protectively identify what data is being stored, where it is located and how it is being transmitted, is crucial. Also defined data/asset owners are essential. With this information, documented risk analysis can be made, vulnerabilities and threats evaluated, simulations made and a localized customization of response plan can be established. With these measures in place, the time to determine if PII is at risk in a given situation, and *breach*

*notification* a requirement, will significantly be reduced. To be GDPR compliant its also necessary to have assigned roles of controller, processor and DPO to take the operative responsibility and provide relevant response plans. Policies and guidelines need to be updated and in accordance with these new responsibilities.

The recent revelations of companies and government agencies being victims of data breaches have shed a light on the importance of proper information security. Not being compliant with GDPR will bring consequences, not only through legal aspects but also financial, process and reputational impact. Being GDPR compliant will in the future be of crucial importance for company reputation. Those companies who are GDPR-compliant will have a competitive advantage when customers select future business partners.

## 7.1 Summary

This thesis has been developed through a thorough examination of different laws, regulations, frameworks and standards. Interviews, forensic investigation and a session at a fintech company have been used as the main sources of knowledge. The obtained conclusions can be summarized as (1) a flowchart of obligations and requirements on *breach notification* depending on the severity of risk of the breach. Figure 5 in Section 5.1.3. (2) a flowchart grouping different kind of breaches into groups based on intrusion points. Figure 6 in Section 5.2.2. Each intrusion point could use similar measures to contain the breach, to make the initial approximation of what data that is exposed. (3) the importance of engagement from top-management. To have a vision and strategy in place for information security. This, to be able to establish the different processes and preventive measures that are of relevance for giving the forensic analyst the best possible starting point.



---

## Future work

---

- Dattainspektionen recently got new demands, changing name to Integritetsskyddsmyndigheten, and adding more support for the GDPR. The authority's mission will be changed so that its supportive and advisory role becomes clearer. This is of interest to follow up on, to see what effect it will have, stricter requirements or more helpful support.
- What has not been covered in this thesis is an evaluation of different tools currently available for log management, IDS, IPS and SIEM systems. These would assist in determining what data may have actually been exposed. This would need a deeper investigation and evaluation for future work.
- An in depth best practice on incident management in compliance with GDPR would be interesting for future work, not zooming in on breach notification but rather focusing on the entire process of incident management.
- Another interesting point for future work is looking at existing laws and aim for a mapping over correlations and conflicts to determine what laws that weight heavier for certain governments and organizations.
- A deeper investigation in log storage could be of relevance to determine an optimal recommendation comparing different cloud solutions with physical solutions.



---

## References

---

- [1] IT-Governance. NIS-directive. Accessed 2017-11-07. [Online]. Available: <https://www.itgovernance.eu/nis-directive/>
- [2] European Commission. Data protection. Accessed 2017-12-05. [Online]. Available: <http://ec.europa.eu/justice/data-protection/>
- [3] M. Johansson. Lagrådsremiss: Ny dataskyddslag. Accessed 2018-01-09. [Online]. Available: <http://www.regeringen.se/4b00ca/contentassets/65ecec1e45b34af0bc1c272e40ccf581/ny-dataskyddslag>
- [4] L. M. Given, *The SAGE Encyclopedia of Qualitative Research Methods*, ISBN: 978-1-4129-4163.
- [5] SANS Institute. PCI DSS. Accessed 2017-11-09. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/compliance/pci-dss-incident-handling-required-before-incident-33119>
- [6] R. Wood Johnson foundation. Qualitative research guidelines project. Accessed 2017-12-07. [Online]. Available: <http://www.qualres.org/HomeInte-3595.html>
- [7] European Commission. Recitals. Accessed 2018-01-02. [Online]. Available: <https://gdpr-info.eu/recitals/>
- [8] ——. General Data Protection Regulation. Accessed 2017-11-07. [Online]. Available: <http://www.eugdpr.org/the-regulation.html>
- [9] ——. General Data Protection Regulation Article-83. Accessed 2018-01-03. [Online]. Available: <https://gdpr-info.eu/art-83-gdpr>
- [10] ——. General Data Protection Regulation Article-33. Accessed 2017-10-05. [Online]. Available: <https://gdpr-info.eu/art-33-gdpr>
- [11] ——. General Data Protection Regulation Article-34. Accessed 2017-10-05. [Online]. Available: <https://gdpr-info.eu/art-34-gdpr>
- [12] ——. General Data Protection Regulation Article-35. Accessed 2017-10-05. [Online]. Available: <https://gdpr-info.eu/art-35-gdpr>
- [13] ——. General Data Protection Regulation Article 4. Accessed 2017-10-31. [Online]. Available: <https://gdpr-info.eu/art-4-gdpr/>

- [14] ——. General Data Protection Regulation Article-9. Accessed 2017-10-05. [Online]. Available: <https://gdpr-info.eu/art-9-gdpr>
- [15] J. Buffington. Breach Notification in Incident Handling. Accessed 2018-01-06. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/incident/breach-notification-incident-handling-2114>
- [16] Article 29 Working party. Guideline on Personal data breach notification under regulation 2016/670. [Online]. Available: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=47741](http://ec.europa.eu/newsroom/document.cfm?doc_id=47741)
- [17] U.S Department of Commerce. Computer Security Incident Handling Guide. DOI: <http://dx.doi.org/10.6028/NIST.SP.800-61r2>.
- [18] SANS Institute. Incident Handlers handbook. Accessed 2017-10-31. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>
- [19] TechTarget. SearchSecurity, computer forensics. Accessed 2017-11-09. [Online]. Available: <http://searchsecurity.techtarget.com/definition/computer-forensics>
- [20] M. Rouse. Confidentiality, integrity, and availability (CIA triad). Accessed 2018-01-02. [Online]. Available: <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>
- [21] National Institute of Standards and Technology. Information Security. Accessed 2018-01-02. [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>
- [22] Myndigheten för samhällsskydd och beredskap. (2016) About MSB. Accessed 2017-11-07. [Online]. Available: <https://www.msb.se/en/About-MSB/>
- [23] Socialdepartamentet. (2015) Lagen, 2015:1052. Accessed 2017-11-07. [Online]. Available: <https://lagen.nu/2015:1052>
- [24] Myndighet för samhällsskydd och beredskap, *Föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter*, ISSN 2000-1886.
- [25] International Organization for Standardization. ISO-standard. Accessed 2017-11-20. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>
- [26] Swedish Standards Institute. ISO 27001 Standard. Accessed 2017-11-20. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>
- [27] Statens offentliga utredningar, *Utredningen om genomförandet av NIS-direktiv*, ISBN 978-91-38-24602-3.
- [28] E. Barker. NIST SP 800-57 Pt. 1 Rev. 4, Recommendation for key management. DOI: <http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4>.
- [29] M. Chapple, D. Gibson, J. Stewart, “CISSP, Certified Information Systems Security Professionals,” ISBN: 978-1-119-04271-6.

- [30] The OWASP Foundation. OWASP top 10. Accessed 2017-11-30. [Online]. Available: [https://www.owasp.org/images/7/72/OWASP\\_Top\\_10-2017\\_%28en%29.pdf.pdf](https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf)
- [31] K. Kent, M. Souppaya. Guide to computer security log management. Accessed 2017-12-15. [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>
- [32] OWASP. Logging. Accessed 2017-10-05. [Online]. Available: [https://www.owasp.org/index.php/Logging\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Logging_Cheat_Sheet)
- [33] PCI Security Standard Council. (2016) Requirements and Security Assessment Procedures. Accessed 2017-11-30. [Online]. Available: [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-2.pdf?agreement=true&time=1512029570186](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1512029570186)
- [34] IBM Research. IBM sets new record for magnetic tape storage. Accessed 2017-12-13. [Online]. Available: <http://www-03.ibm.com/press/us/en/pressrelease/52904.wss>
- [35] SBS CyberSecurity. (2017) Equifax Lessons Learned. Accessed 2017-10-05. [Online]. Available: <https://sbscyber.com/portals/0/documents/sbs2017-equifaxbreach.pdf>
- [36] Panda Security. NotPetya returns as Bad rabbit. Accessed 2017-12-13. [Online]. Available: <https://www.pandasecurity.com/mediacenter/pandalabs/notpetya-bad-rabbit/>
- [37] The Guardian. Ashley Madison breach. Accessed 2018-01-019. [Online]. Available: <https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports>
- [38] Working party 29. Opinion 03/2014 on Personal Data Breach Notification. Accessed 2017-12-15. [Online]. Available: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf)





---

## GDPR Article 4 – Definitions

---

This section is directly copied from the relevant definitions of Article 4 in GDPR.  
*For the purposes of this Regulation:*

- 1. *‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
- 2. *‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*
- 7. *‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*
- 8. *‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*
- 11. *‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*
- 12. *‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*
- 22. *‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;*



---

**Art. 33 GDPR**

**Notification of a personal data  
breach to the supervisory authority**

---

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with [Article 55](#), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
  - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - (c) describe the likely consequences of the personal data breach;
  - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.



**Art. 34 GDPR**  
**Communication of a personal data  
breach to the data subject**

---

- (1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
- (2) The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of [Article 33\(3\)](#).
- (3) The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
  - a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
  - b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
  - c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
- (4) If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.



---

**Recital 86**

**Notification of data subjects in case of data breaches\***

---

The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.





---

## Questions for qualitative interview

---

Questions discussed at fintech company:

- What processes do you have for incident response today?
- Have you identified what systems containing personal data?
- Inventory of assets?
- Internal data or outsourced data, cloudbased?
- How many has access to the personal data? (principle of least privileged)
- What personal data do you have?
- Is there a corporate policy in place for managing logs? (how the logs are captured, stored, analyzed)
- Is there a defined retention policy for logs over the organization?
- Are logs being stored centrally?
- If not, how are they stored?
- Do you have an Incident manager, security incident manager?
- Are there backups of logs?
- Are the logs encrypted?
- Is any personal data being stored in the logs?
- Is data encrypted at rest resp in motion?
- What intrusion detection systems are being used?
- Do you use Data Loss Prevention?
- What is being logged? (server workstation operating logs, applications logs, security tool logs, outbound proxy logs)
- Have the employees been doing any security training?
- If a data breach would occur today, what would you do?



**LUND**  
UNIVERSITY

Series of Master's theses  
Department of Electrical and Information Technology  
LU/LTH-EIT 2018-616

<http://www.eit.lth.se>