General data protection regulation compliance at SMEs: guideline, incident response methodology, information security controls, and case company evaluation

Olawale Michael Obanla and Aleksei Sapozhnikov

2019 Laurea

Laurea University of Applied Sciences

General data protection regulation compliance at SMEs: guideline, incident response methodology, information security controls, and case company evaluation

Olawale Michael Obanla and
Aleksei Sapozhnikov
Security Management
Bachelor of Business Administration
Bachelor's Thesis
May, 2019

Laurea University of Applied Sciences **Abstract**

Security Management
Bachelor of Business Administration

Year 2019 Pages 63

A multitude of small and middle enterprises are struggling to attain compliance with the General data protection regulation (GDPR) and it can be a challenge for companies to comprehend all the legal requirements. The purpose of the thesis was to help organizations understand the requirements of the Regulation, how data breach notification should be processed, and how to resist the incidence of data leakages caused by staff errors. The aim of the thesis was to create a GDPR guideline, GDPR personal data breach notification plan and form, to discover what are the most important information security controls regarding data leakages caused by staff errors; also, based on the research results, to evaluate the case company to encourage further development of information security system.

This work used the General data protection regulation as the main source of information to build a knowledge base for the thesis. Legal literature was used to define what compliance is, what are the stages of regulatory compliance development, and how compliance can be developed in organizations. Professional literature and research articles were reviewed on such themes as information security management, risk management, and incident management, particularly ISO/IEC 27005 standard of 2018 and National Institute of Standards and Technology publications. InfoWatch report was examined to find information security controls that can consolidate the information security system of a company against most common data leakage types caused by staff errors.

To answer the research questions a thematic analysis of theoretical framework was used to create a simple structure for a guideline, data breach notification plan and form, and to find the most important information security controls against data leakages caused by staff errors. To construct a complete picture of how the case company approaches the requirements of the law, a semi-structured interview was conducted. The interview structure was framed on the research questions and their results, so that the questionnaire had three topics based on the GDPR guideline, data breach notification form and plan, and findings on information security controls.

The research results were reflected in the GDPR guideline, personal data breach notification plan and form, and additionally the research work defined the most important information security controls against data leakages caused by staff errors. The given work made an evaluation of the case company and proposed development measures towards fostering greater regulatory compliance and enhancing information security culture. The case company was presented with the development proposals and is developing its information security culture on the basis of the results of the evaluation.

The given work answers all three research questions and the results can be used by SMEs to prepare for the GDPR, personal data breach notification procedures, and to protect themselves against most common data leakage types caused by staff errors.

Keywords: GDPR compliance, data breach notification, information security risk, personal data processing, information security controls

Table of Contents

List of abbreviations

CIA	Confidentiality, integrity, availability
DLP	Data loss prevention
DPD	Data protection directive
DPO	Data protection officer
EC	European Commission
GDPR	General data protection regulation (the Regulation)
ISMS	Information security management system
NGO	Non-governmental organization
NIST	National Institute of Standards and Technology
RPO	Recovery point objective
RTO	Recovery time objective
SDO	Service delivery objective
SME	Small and medium-sized enterprises

List of definitions

Definitions used in this thesis, taken from General data protection regulation.

"'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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", Article 4 (1);

"'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", Article 4 (2);

"'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person", Article 4 (5);

"'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", Article 4 (7);

"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller", Article 4 (8);

"'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", Article 4 (11);

"'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" Article 4 (12);

"'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51", Article 4 (21);

"'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries", Article 4 (26). (European Union, 2016)

1 Introduction

The lengthy process of a new set of legislation aimed at reforming the legal framework to safeguard the private life rights and personal data of European Union (EU) residents was completed in December 2015.

On 27 April 2016, the European Commission (EC) endorsed the General data protection regulation (GDPR or Regulation). The Regulation was adopted into EU law on 25 May 2018 and replaced the EC legislation Data protection directive (DPD) of 1995. DPD 95 was the first decree of that type for private data protection in EU of the scale, which legally covered all EU member states. (European Union, 1995) One notable distinguishing feature between the Regulation and the DPD is that the GDPR automatically becomes law in each of the member states, whereas application of the DPD varied depending on a given member state. The GDPR sought and can aptly be regarded as a harmoniser of all existing laws on personal data protection in the EU.

Whilst the emphasis is often on the rights of the data subject when discussing the GDPR, it is important to remember that the EC is also trying to facilitate organizations to share personal data within the EU, recital (6). (European Union, 2016)

The Regulation concerns the personal data of EU citizens wherever that data is held, says Article 3(1). (European Union, 2016) This means that if an organization is not based in the EU but has customers, suppliers and other parties within it whose data a company holds, the GDPR applies to that company. Leading on from this, if an organization does not look after that data in the way the GDPR requires, it may be subject to the penalties that the Regulation allows, Article 83. (European Union, 2016) These penalties have been increased significantly from previous legislation. If an organization does experience a breach of personal data, it has no choice but to notify the supervisory authority, Article 33. (European Union, 2016)

The mainstay of what the GDPR is about forcing organizations to take the protection of the personal data of EU citizens seriously. Personal data protection is a right of all citizens, Article 8 of Chapter of Fundamental Rights of European Union. (European Union, 2012)

1.1 The purpose and aim

When new regulations are being enforced into law, many organizations find it difficult, especially small and medium sized enterprises (SME). SMEs often ask how to be compliant with the GDPR, what are the main principles of the Regulation, what should be done in case of a data breach, who should they notify, what authority, in what manner should the notification be processed, when should the data subject be notified, how should the notification be drafted, and so forth.

This research builds on the knowledge of existing regulation and how an organization should handle personal data breaches, helping readers who might not be familiar with GDPR to learn what its implementation looks like. The purpose of the thesis work is to assist organizations to understand the requirements of the GDPR, how data breach notification should be processed, and how to resist the occurrence of data leakages caused by staff errors.

The aim of the thesis is to create a GDPR guideline, personal data breach notification plan and form, to discover what are the most important information security controls regarding data leakages caused by staff errors. The thesis also aims to evaluate the case company, based on research results, to encourage further development of information security system. The case company is a Helsinki based small enterprise which works in the field of consulting.

1.2 Research questions and methods

Below are the research questions that are used to guide this investigation:

1) What are the requirements for SME to be compliant with the GDPR?

2) What are the obligations of an organization to notify authorities communicating a data breach?

3) What are the controls to mitigate the risks of most common data leakage types caused by staff errors?

To answer the research questions a thematic analysis of theoretical framework will be carried out. This will help to create an easy to understand structure for a guideline, data breach notification plan and form, and to find the most important information security controls against data leakages caused by staff errors.

A semi-structured interview with a case company representative will be conducted to find out how the case company approaches the requirements of the Regulation. The research questions and their results will shape the interview structure, so that the questionnaire will consist of three topics based on the GDPR guideline, data breach notification form and plan, and findings on information security controls.

1.3 Limitations

The given work focuses on information security management rather than cybersecurity and its technical details.

The guideline is based on 7 main principles of Article 5 and recommendations on codes of conduct of Article 40. This guideline is suitable for non-governmental organizations (NGO), SMEs, and non-international organizations. The GDPR has stipulations on conditions and

restrictions when dealing with special categories of personal data (“sensitive data”). International companies, organizations that process “sensitive data” or process personal data on a large scale are not considered in the given work. See paragraph 2.1.5 on what special category of data is.

1.4 Outline

This study is structured in five chapters. The first chapter is an introduction of the study; the background of the study is presented together with the objective of the research with its limitations. A theoretical framework describes theories of the GDPR, compliance development, ISO/IEC 27005:2018 standard, NIST publications, data breach, and InfoWatch report regarding most common data leakage types caused by staff errors in chapter two. The third chapter explains the methodology used in research and development. The fourth chapter discusses the results of the research and development. The fifth chapter contains the conclusions of the study.

2 Theoretical framework

This chapter consists of theories of the GDPR in paragraph 2.1, compliance development in 2.2, information security and risk management in 2.3, and incident management in 2.4.

2.1 General data protection regulation

The GDPR document itself consists of 88 pages divided into two main parts: Recitals - 173 numbered paragraphs explaining the principles and intent of the regulation. Article 99 - Parts of the details of the Regulation - this is the part to be observed. The regulation seeks to protect the fundamental rights and freedoms of natural persons, and the right to protection of personal data, recital (1). (European Union, 2016) Such as the right to be erased and forgotten, and the right to request data portability and clear consent for processing personal data, Article 17. (European Union, 2016) GDPR also restricts companies and organizations from storing personal data for a longer time than necessary, prohibiting storage of data that is not relevant to their business and enforce penalties if not done accordingly, Article 5. (European Union, 2016) Article 83 expresses that the competent supervisory authority (see the definition below) will make an assessment “in each individual case” when deciding whether to impose an administrative fine. (European Union, 2016)

2.1.1 Supervisory authorities

Each country within the EU will have a supervisory authority which is responsible for overseeing the operation of the GDPR in that country, Article 51 (1). The GDPR establishes the European Data Protection Board (the ‘Board’) supervisory authority, in Article 68 (1), to oversee how the Regulation is applied in the EU members’ states, Article 70 “Tasks of the board”. Each country supervisory authority has a seat on the Board, together with the head of the European Data Protection Supervisor, Article 68 (3). The Board must produce an annual report on data privacy rights to tell the general public of EU member countries the current state of the adherence to the law, claims Article 71 (1). (European Union, 2016)

2.1.1 Article 5 and main principles

The GDPR establishes a number of principles in Article 5 “Principles relating to processing of personal data” that underpin the legislation and are outlined using the following terms. (European Union, 2016)

1) Incident, fairness, and transparency. Companies should process all personal data legally and fairly. Meaning that all the controllers and processors need to say in clear terms what they are going to do with the data. (European Union, 2016)

2) Purpose limitation. The Regulation requires that organisations can utilize the processed data only according to the purposes stated and agreed between the controller (processor) and data subject in the consent. (European Union, 2016)

3) Data minimization. A controller cannot collect more personal data than it needs. (European Union, 2016)

4) Accuracy. Controllers (processors) must keep personal data up to date and deal with inaccuracies as soon as they have been found. (European Union, 2016)

5) Storage limitation. Companies cannot keep personal data for a longer period than it is necessary. (European Union, 2016)

6) Integrity and confidentiality. Controllers must apply appropriate safeguards to keep personal data safe. (European Union, 2016)

7) Accountability. One needs to be able to show that a company complies with the principles mentioned above. (European Union, 2016)

2.1.2 Personal data processing

For the processing of personal data to be lawful, it must meet at least one of a number of criteria, and an important first step in considering a company processing activities is to clearly establish which of the criteria applies in any given situation. In essence, the criteria to choose from with regard to the lawfulness of the processing are, as stated by Article 6: the data subject has consented to it; it is needed to perform a contract between an organization and the data subject, or to see whether a contract can happen; an organization legally have to do it; data controller is protecting the vital interests of the data subject; it is in the public interest; it is for an organization's legitimate interests – as long as it does not affect the data subject's rights and freedoms. (European Union, 2016)

2.1.3 Controller's responsibilities

Article 24 sets general obligations on controllers. They are required to implement adequate measures to ensure compliance with the law and its stipulations. In accordance to the volumes of processing personal data controllers must engage data protection policies in practice. Adherence to the Regulation can be shown with the help of approved certification or approved codes of conduct. (European Union, 2016)

GDPR Article 25 addresses the need for data privacy by design and default. The controller needs to use both managerial and technological methods ensure that processing data meets compliance with the principles of GDPR. (European Union, 2016)

As stated in Article 26, in where there are two or more controllers processing data together they are obligated to processing data as joint controllers. The processing of data shall be done according to the regulation with corresponding duties of controllers. (European Union, 2016)

The security of processing of data must be taken into consideration as stipulated in Article 32. It is required for both controllers and processors of personal data to ensure the implementation of the adequate safeguards commensurate to the risks. The controller and the processor are required to use security methods such as pseudonymization and encryption, to provide confidentiality, integrity, availability (CIA) of information security, and to ensure timely restoration and availability of personal data after an incident. These methods should be regularly tested and evaluated to make sure they meet the effectiveness of technological and managerial measures of security. (European Union, 2016)

According to Article 37, depending on the organization and what it does with personal data, a controller may need to designate a data protection officer (DPO). An organization will have to designate one in case if a company is a public authority or body, if a company monitors data subjects on a large scale or if large volumes of special category (‘sensitive data’, see paragraph 2.1.5) data are involved. Article 37 (3) stipulates, that a shared DPO can be assigned in cases when organizations sizes are not large. The DPO is the main contact with the supervisory authority when key issues of data privacy and protection are addressed to the organization. In order to fulfil the role, the DPO must be competent in and have practiced application of data protection law. (European Union, 2016)

2.1.4 Codes of conduct and certification

Adherence to the GDPR can be demonstrated by the means of approved codes of conduct and approved certification mechanism, states Article 24 (3). (European Union, 2016)

According to Article 40 “Codes of conduct” (1), the Regulation makes provision for EU member states and supervisory authorities to induce associations of data controllers and processors creating relevant codes of conduct. Approved codes of conduct can be used to help controllers (processors) comply with the Regulation. (European Union, 2016)

Codes of conduct should address the following aspects of the Regulation, Article 40 (2): fairness and transparency of data processing, legitimacy of data processing, process of collection of personal data, pseudonymisation of personal data when it is required, information disclosure to the public or a data subject, abiding to the rights of data subjects, protection for children and parental responsibility regarding personal data processing, security of processing of personal data, personal data breach notification to authorities and individuals, international transfers of personal data. (European Union, 2016)

According to article 42 (3), certification can be obtained from a competent certification body. EU member states and relevant data protection bodies shall prompt to create certification mechanisms. Certifications are valid for three years. (European Union, 2016)

2.1.5 Personal data

It can be inferred from the definition in Article 4 (1) of what personal data is. That is any information on a particular person, with the help of which it is possible, whether directly or indirectly to identify the individual. The regulation establishes that the category of personal data can include names, identification numbers, online identifiers, and all information related to “physical, physiological, genetic, mental, economic, cultural or social identity” of a person. (European Union, 2016)

An individual can be identified by information from private, professional or public life. Here are some examples from The International Association of Privacy Professionals (IAPP) Infographic “Categories of Personal Information”. These are internal personal information (knowledge and belief, authenticating, preference), external personal information (identifying, ethnicity, sexual, behavioural, demographic, medical and health, physical characteristics), historical personal information (life history), financial personal information (account, ownership, transactional, credit), social personal information (professional, criminal, public life, family, social network, communication). (IAPP)

It is important to make a distinction between data processing between personal data and sensitive personal data to be able to incorporate adequate security measures. According to Article 9 (1), controllers (processors) are prohibited to process special categories of data (“sensitive data”). It includes the data related to origin, political opinions, beliefs, trade union membership, genetics, biometrics, health, and sex life. This rule is not applied in cases, described in the stipulation (2) of Article 9, when a data subject has given a consent for specified purposes. (European Union, 2016)

2.1.6 Consent

If one believes that one’s processing is lawful because of the existence of the data subject’s consent, then one must be able to prove it, Article 7 (1). A person cannot hide the consent wording amongst other contractual ramblings and expect to get away with it either. It must be in an “intelligible and easily accessible form, in clear and plain language” says Article 7 (2). Otherwise, the consent doesn’t count, and the processing could be judged to be unlawful. (European Union, 2016) Once given, the consent can be withdrawn at any time by the data subject and this must be as easy to do as it was to give it in the first place, Article 7 (3). (European Union, 2016)

The Regulation makes a provision in Article 8 for a child consent as well. A child must be at least sixteen years of age to be able to give consent (younger if a member state decides so, with a lower limit of thirteen) otherwise parental consent must be obtained, Article 8 (1). (European Union, 2016)

2.1.7 Rights of the data subject

According to Article 12 (3), the controller holding their personal data must react and respond to a request from a data subject within a month to two months. The required period depends on the number of data subject requests. The GDPR establishes the following set of rights that the data subject can exercise. The right to be informed, being told what data will be collected, why, by whom, for what purpose and where the data will go, Articles 13 and 14. The right of access, being able to view personal data that is held on the data subject, Article 15. The right to rectification, getting the data corrected if they are wrong or inaccurate, Article 16. The right to erasure, having personal data removed when they are no longer in use, Article 17. The right to restrict processing, pausing the processing of the data if there are grounds to do so, Article 18. The right to data portability, obtaining the data in a transportable form and moving it to an alternative processor, Article 20. The right to object, stopping the data from being processed, Article 21. Automated decision making and profiling, having a human involved in important decisions, Article 22. (European Union, 2016)

Article 77 of the Regulation provides a right of data subjects to report to supervisory authorities on violations of the law. Data subjects can lodge a complaint with the relevant supervisory authority directly themselves or may use the services of a not-for-profit body active in the field of data protection, says Article 80 “Representation of data subjects”. (European Union, 2016)

2.1.8 International transfers

The Regulation makes provisions for international transfers of personal data. An international processing of personal data shall comply with the GDPR stipulations of Chapter V “Transfers of personal data to third countries or international organisations”, Article 44. (European Union, 2016). Controllers and processors are required to maintain a certain level of data privacy protective measures transferring data internationally.

The Regulation establishes in Article 46 (2) the means by which the controllers and processors of international organizations can ensure implementation of appropriate safeguards: a legally binding agreement (between public bodies only), binding corporate rules, using standard clauses in contracts, signing up to an approved code of conduct or certification scheme. (European Union, 2016)

As a result of the Regulation enforcement, non-EU member states controllers and processors of personal data of EU residents must be GDPR compliant.

2.1.9 Penalties

According to Chapter VIII "Remedies, liabilities and penalties", the fines that can be levied for non-compliance with the GDPR are certainly larger than those for the Directive it replaces. The recital (148) claims there are fines that can be imposed if an infringement of the law has occurred or a reprimand can be given to a controller or processor. According to Article 83 (2), the demanded fine depends on a wide variety of factors, including the type and quantity of personal data involved, how hard the culprit organization tried to protect the data, presence of a certification, codes of conduct, and breach notification particularities, how much they co-operated with the investigation and the specific article(s) of the GDPR they are judged to have contravened. (European Union, 2016)

According to Article 83 (4,5,6), fines allowable are up to 2% of global turnover or ten million euros for lower level infringements and up to 4% of global turnover or twenty million euros for more serious cases. (European Union, 2016)

The EU Member States can set the law stipulations which impose criminal penalties. They are applied in case of violation corresponding national rules covered in the GDPR, from recital (149). (European Union, 2016)

2.1.10 Data breach notification

In accordance with the GDPR, a breach must be communicated to the supervisory authority within 72 hours after having become aware of the breach, and affected individuals must be notified if the severity so requires, Articles 33 (1) and 34 (1) respectively. In case of delay of breach notification, a controller shall provide evidence for the reasons of the delay to the supervisory authorities to prove that. (European Union, 2016)

The followings are required for the notification, Article 33 (3): basic description, the scale of the data breach; DPO's and other relevant persons' names and contact details; expected data breach outcomes; description of the measures a company is going to take or have already taken to handle the data breach and mitigate possible consequences and future risks. (European Union, 2016)

According to Article 33 (5), all the relevant information regarding data breach shall be documented. It includes facts about the personal data breach, measures taken to recover and data breach consequences. (European Union, 2016)

In the likelihood of high risks to the rights of data subjects, a controller shall notify data subjects without undue delay, as states Article 34. In case when the controller has not met

the obligation of communicating, the supervisory authority may require the controller to inform data subjects about the breach. (European Union, 2016)

2.1.11 Compliance in GDPR

Recital (2) of the GDPR states “The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.” Thus, the Regulation is based on the principles of respect of fundamental human rights with the aim to protect a natural person’s data in the EU. From the recital (11), “Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.” (European Union, 2016)

2.2 Compliance development

Oxford Dictionaries defines the word compliance as “The action or fact of complying with a wish or command” or “The state or fact of according with or meeting rules or standards”. (English Oxford Living Dictionaries, n.d.)

2.2.1 Regulatory and compliance development

Compliance from a perspective of regulators. David Jackman proposes a model called “General model of regulatory and compliance development”. It is divided into 5 stages and has a graph represented in Figure 3. These are start-up, crises, expansion, sustainability, outcomes-led stages. (Jackman, 2015, p. 8) The graph is an arctangent curve meaning that there is always a level where compliance cannot get hire above a certain level of maturity.

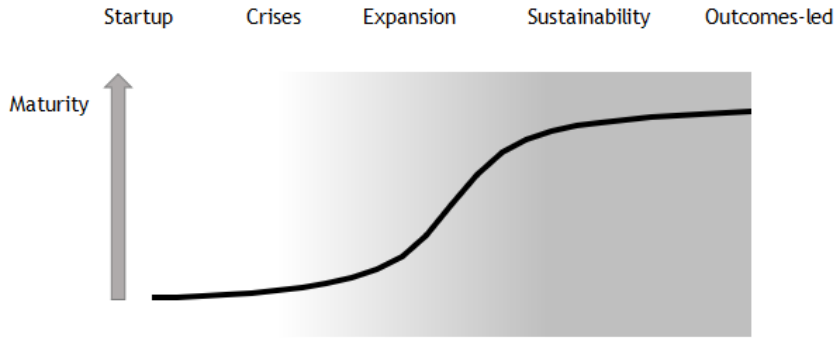


Figure 1: General model of regulatory and compliance development (Jackman, 2015, p. 8)

The phase of start-up is the beginning of the introduction of the legislative practices. Regulators set requirements onto the businesses addressing certain problems in a society or an industry. The second stage is related to the responsiveness of businesses to a law enforcement. Companies and regulators start to think about how to address those problems. This stage of the regulation development has such properties as lack of organization and an irrational approach to filling the gaps between current and desired compliance levels. During the stage of expansion, the regulation sets more clear goals compared to the previous stages of the development, enhances its grip and gets mature. The fourth stage includes maintenance of compliance level and its improvement to its limits. The last stage is outcomes-led, which emphasizes the results of regulation implementation. Impact assessment helps to understand the causes and effects of the enforced regulation. This fortifies future creativity in a systematic and holistic approach in regulation and compliance. (Jackman, 2015, pp. 8-9)

The maturity level of corporate compliance. There are 5 stages in maturity development.

Table 1: Levels of corporate maturity (Jackman, 2015, pp. 189-191)

Level N	Maturity level description
Level 1 Noncompliance	Unawareness or reluctance of necessary introduction of compliance amendments into the corporate structure and policies
Level 2 Minimum standards	Inchoate stages of compliance or little compliance Culture: negligence; unwillingness to spend resources for compliance, take responsibilities, make decisions. Compliance: superficial policies, primary licensing, high standards of regulators cannot be met by industries.
Level 3 Compliance culture	Basic frameworks of compliance are applied. For the most part, it is an expensive and least cost-effective stage for a company processes compliance. Culture: ill-conceived compliance; no proactive steps; bureaucracy; no will of compliance from within. Compliance: high costs of regulation; weak levels of awareness, reporting and governance; dependency on audits.
Level 4 Business improvement	Existing compliance is seen as a value. A company wants to improve its business goals through compliance. Culture: focuses on risks; culture considered as a supportive measure, ethical culture introduced into most business levels. Compliance: gained outcomes; mitigated risks resulting in good reputation.

Level 5 Values-led	A company naturally aims to be compliant. Compliance is based on the values of a company culture. Culture: focuses on values and outcomes; implemented core values at all levels of an organization, personal responsibility; includes training, awareness, and ethics. Compliance: trusted relationships, built-in ethical culture, stable regulation, strong risk control, lower cost, creates trust.

The level of compliance in a corporate sense increases independently from the "General model of regulatory and compliance development". However, the same processes prompt both company compliance and regulatory compliance to grow. (Jackman, 2015, p. 192)

Introduction of legislative practices sets a question before all companies how to be compliant with a regulation. If a company is not aware of the requirements most likely it is not compliant with the regulation. It brings a company to the position of start-up or crises according to the stages of regulation of David Jackman. (Jackman, 2015, p. 189) Major changes are to be introduced into the organizational processes to expand and sustain compliance with the law. The outcomes of compliancy with the law are increased level of reputation among public and businesses and reduced risks of fines. (Jackman, 2015, pp. 189, 192)

2.2.2 Techniques of regulation and methods of compliance improvement

Laws usually offer reward in case of compliance, otherwise, sanction penalties. (Friedland, Sanctions and Rewards in the Legal System : A Multidisciplinary Approach, 1989, p. 12). There are different techniques which a regulator can use to make companies comply with a law. Legislators employ, for example, licensing, rewards, different forms of liability, and so on. (Friedland, Securing Compliance : Seven Case Studies, 1990, p. 10).

From a perspective of companies who need to comply with a specific law, there are following methods of compliance performance improvement: risks-based compliance, cost-benefit based analysis, principles-based method, and prevention method (applying corporate culture, ethics and governance tools). (Jackman, 2015, p. 9)

2.3 Information security and risk management

In this chapter confidentiality, integrity, and availability of data (CIA triad) and ISO/IEC 27005 information security risk management standard are reviewed.

It is important to be able to distinguish the differences between prevention and response terms in information security management. A strong security system is built upon a balanced system of prevention and response mechanisms. (Jajodia, 1999, pp. 71-75) Prevention is based on past experiences, whereas response is planning for the unknown future or unexpected incidents. (Kendall, 2005, pp. 1001-1012) See Figure 2 below of the prevention and response model. (Baskerville, 2014)

Subparagraph 2.3.2-2.3.4 reviews the ISO/IEC 27005 standard which is related to risks

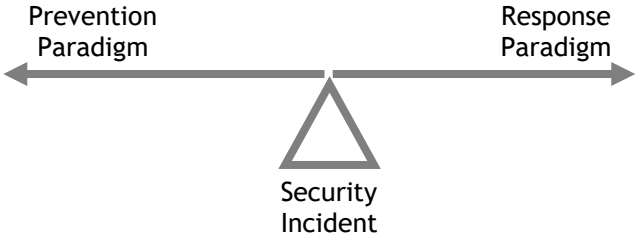


Figure 2: Prevention and response model (Baskerville, 2014)

analyses and prevention of incidents, respectively touching on prevention paradigm. In the next paragraph 2.4 incident handling and response concepts are reviewed, which are related primarily to the response paradigm.

2.3.1 CIA triad

The level of security systems is usually measured based on the confidentiality, integrity, and availability (CIA) triad. Each of the components must be considered while developing an information security system and they are important elements of information security. Depending on the organisation type and respectively its goals of information security management these three principles can be balanced. Information security objectives are to protect assets from the perspectives of confidentiality, integrity, and availability. (Stewart, 2012, pp. 3, 214)

Integrity means “guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity”; confidentiality means “preserving authorized restrictions on access and disclosure, means for protecting personal privacy and proprietary information”; and availability “means ensuring timely and reliable access to and use of information”. (Federal Information Security Modernization Act of 2014, p. 128)

2.3.2 ISO/IEC 27005:2018. Information security risk management

Information security risk management is an integral part of an information security management system (ISMS), continuous process of managing vulnerabilities and risks that may have a negative impact on an organization.

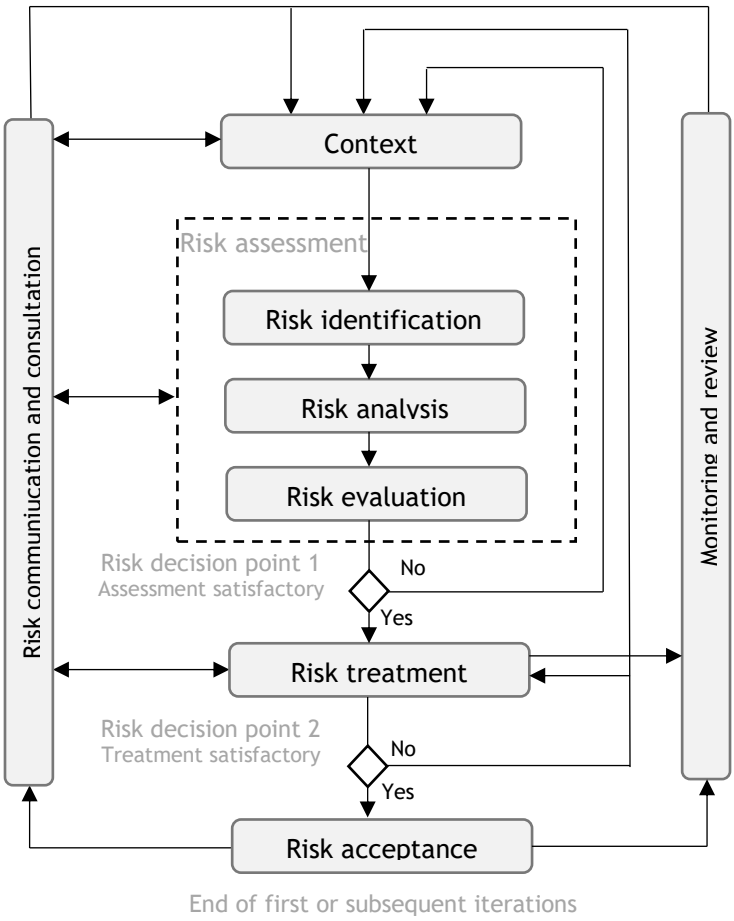


Figure 3: Information security risk management process (ISO/IEC 27005, 2018, p. 9)

The process of information security risk management (see Figure 3) of an organization establishes the context, analyses the risks and finds appropriate safeguards to mitigate the risks. (ISO/IEC 27005, 2018, p. 7)

Information security risk management is an important part in the context when developing ISMS, legal compliance, incident response plan, business continuity plan, and information security requirements for a product or service. (ISO/IEC 27005, 2018, pp. 10,11)

2.3.3 Risk assessment in ISO/IEC 27005:2018. Risk assessment scale

To start the information security risk assessment, it is required to define minimum requirements, limitations, and organization. To carry out information security risk assessment the risk must be identified, quantified and qualified according to the organization objectives.

(ISO/IEC 27005, 2018, p. 13) Risk assessment results in the ascertainment of the value of information assets, recognizes the threats and vulnerabilities that are present, it also recognizes the controls, effects, and consequences. Conducting risk assessment can be done in two or more stages. The high-level assessment is first performed to determine a potential high risk that needs further assessment. (ISO/IEC 27005, 2018, p. 14)

Risk assessment consists of activities such as risk identification, risk analysis, and risk evaluation in the order as shown in Figure 3. (ISO/IEC 27005, 2018, p. 9)

Risk identification allows gaining a better view of what can cause a loss. It recognizes assets, threats, controls, vulnerabilities, and consequences considering internal and external factors (ISO/IEC 27005, 2018, pp. 14-17). All the data gathered is considered when processing the next step of risk analysis. Risk identification examines all possible threats regardless of whether an organization has appropriate controls or not. (ISO/IEC 27005, 2018, p. 14).

Risk analysis includes gathering and recording of data related to threats from internal and external factors, also detecting the risk sources and its impact on an organization. The methodology for risk analysis can be qualitative or quantitative. (ISO/IEC 27005, 2018, p. 17) Qualitative analysis is used to determine the level of the likelihood, the potential consequences. Consequences can be divided into low, medium, and high levels. Quantitative risk analysis is used in scaling values of numbers from both consequences, and the possible likelihood from data gathered from sources. Numerical accuracy and validity of the model used in risk analysis define the quality of quantitative risk analysis. Analyses usually are based on data from previous incidents. The disadvantages of quantitative analyses are not being able to determine new or emerging risks or lack of data on past incidents. (ISO/IEC 27005, 2018, p. 18)

Risk evaluation includes making decisions concerning risks and prioritizing of risks, threats, and vulnerabilities in terms of their severity and risk treatment options. For example, in cases of low-value information assets, the risks may be accepted without devising security controls and countermeasures. On the other hand, for high-value assets, security controls and countermeasures are devised, and proper risk treatment strategies are employed. (ISO/IEC 27005, 2018, p. 20)

Correlations between threats occurrence likelihood and levels of adverse impacts can be analysed with the help of the following risk levels assessment scale (NIST Special Publication 800-30, 2012, pp. I-1)

Likelihihood of threat event occurence	Level of impact				
	Very low	Low	Moderate	High	Very high
Very high	Very low	Low	Moderate	High	Very high
High	Very low	Low	Moderate	High	Very high
Moderate	Very low	Low	Moderate	Moderate	High
Low	Very low	Low	Low	Low	Moderate
Very low	Very low	Very low	Very low	Low	Low

Figure 4: Risks assessment scale (NIST Special Publication 800-30, 2012, pp. I-1)

Further risk treatment measures are taken based on the risk matrix. (Taylor, 2013, p. 26)

2.3.4 Risk treatment in ISO/IEC 27005:2018

According to ISO standards 2018 there four risk treatment types which are risk modification, risk retention, risk avoidance, risk sharing. (ISO/IEC 27005, 2018, p. 21) Alternatively, risk modification, risk transfer, risk avoidance, and risk acceptance. (Taylor, 2013, pp. 26-27)

Risk modifications include three variants. These are reducing the threat, the vulnerability, or the impact of a risk. (Taylor, 2013, p. 27) Employing and changing of appropriate controls helps an organization to manage the risks. Controls assist an organisation to implement such security measures as awareness, correction, detection, deterrence, elimination, impact minimization, monitoring, prevention, and recovery. (ISO/IEC 27005, 2018, p. 22)

Risk transfer is the method of moving potential risk to a third party. (Taylor, 2013, p. 27) The examples of sharing risks are an insurance or a third company that provides information security services. (ISO/IEC 27005, 2018, p. 24)

Risk avoidance or termination method means not doing an activity that involves a risk. (Taylor, 2013, p. 26) Also, an organization can change the operating environment or conditions to avoid risks. (ISO/IEC 27005, 2018, p. 23)

Risk acceptance is involved when a potential risk has a low impact the organization is willing to accept the consequence that may come with it. (Taylor, 2013, p. 27) The acceptance of risk is determined depending on the severity level of the risk. (ISO/IEC 27005, 2018, p. 23)

2.3.5 Information security controls.

Security controls can be divided into two which are technical and nontechnical. Technical controls secure the assets of the organization using computer software and hardware.

Nontechnical controls are operational and managerial. (NIST, 2002, p. 20) Information security controls help an organization to protect CIA of information and manage information security risks. (NIST, 2002, p. 22) Security controls can be divided into two categories. These are preventive controls and detective controls. (NIST, 2002, p. 20)

Preventive controls help an organization to foresee and take appropriate measures before an unwanted incident happened. Data encryption and access control are examples of detective controls. (NIST, 2002, p. 20)

Detective controls help recognize and find the attempted infringement of security of an organization. Detective control alerts when there is a need to take actions against violations. Audit trails and intrusion detection tools are examples of detective controls. (NIST, 2002, p. 20)

Optimal risk management of an organization combines deterrence, avoidance, prevention, detection, recovery, and correction controls. (NISTIR 7298, 2013, p. 173)

2.4 Incident management

This chapter will cover incident handling, incident lifecycle map of National Institute of Standards and Technology (NIST), threats to information security, and recovery objectives after an incident activity. It is worth noting that professional literature uses the terms incident management, incident response, and incident handling interchangeably.

Incident handling is the service which includes the processes related to security events and incidents. (Johnson, 2014, p. 11) The functions of incident handling are discussed in more detail below.

2.4.1 Threats

Threats can be categorized based on their origin into external and internal, and threat agents are natural, human, and environmental. (Jouinia, 2014, p. 494)

An internal threat occurs when an individual who has authorized access to network area and misuses the resources of an organization deliberately or indeliberately. (Jouinia, 2014, p. 494) Such a threat can result in disclosing sensitive information to outsiders. (Probst, 2010, p. 23) An external threat comes from persons outside of an organization or natural disasters. Violators do not have authorized access to the network areas and premises. (Jouinia, 2014, p. 494)

Natural disasters, such as earthquakes, floods, fires, cyclones, and epidemics can result in threats to an organization's information assets. Natural disasters can be of varying types depending on their location and occurrence. Some may occur frequently, while others may

occur after a long period of time. These threats are difficult to guard against because they are difficult to predict but can have a severe impact on business. (NIST, 2002, p. 35)

An organization may face human-made threats, such as identity theft, fraud, phishing attacks, denial-of-service attacks, and damage by employees with malicious intentions. Also, unintentional acts of men, for example, error or negligence, can cause damage to information systems. Man-made threats can be identified and controlled with the help of proper planning. (NIST, 2002, p. 35)

Technological threats can occur due to malfunctioning or failure of an information system, such as computer hardware or software. Some other technical threats include power outage, network failure, and loss of utility services. (Jouinia, 2014, p. 494)

The development of a response plan should be based on the results of a business impact analysis. This analysis helps you to prioritize risks based on their impact on business operations. (NIST, 2002, p. 21)

2.4.2 Data breach

Fowler defines security incident as “an event that violates organizational, regulatory, legislative or contractual security, or privacy policies”, and data breach as “a security incident that: involves the intentional or unintentional access, disclosure, manipulation or destruction of data; or meets specific definitions of a “Breach” as per state/province or federal laws or active contracts with clients, third parties or partners”. (Fowler, 2016, p. 2)

The origins of data breaches can be cybercrime, errors, and omissions, also, third parties outsourcing services and products. (Fowler, 2016, pp. 1,19)

A data breach can be broken down into several stages. The breach lifecycle looks as follows in Figure 5. (Fowler, 2016, p. 3)

Figure 5: Data breach lifecycle (Fowler, 2016, p. 3)

It is important to note the 8th stage of the lifecycle which is notification and inquiry management. At this stage, it is necessary to notify victims of the data breach and regulators about the occurred accident. (Fowler, 2016, p. 5)

2.4.3 Incident handling and response

NIST proposes six stage incident response plan for handling incidents. See Figure 4. The incident response team has to be set up in the very beginning of incident handling lifecycle, equipped with appropriate resources. (Special Publication 800-61, 2012, p. 21)

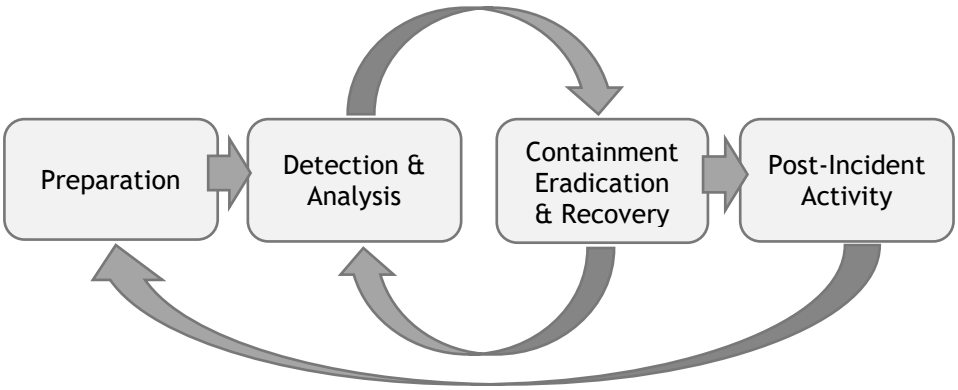


Figure 6: Incident handling lifecycle (NIST Special Publication 800-61, 2012, p.

During the preparation stage, preventive measures are taken. It includes the implementation of all the necessary tools to limit incidents occurrence. Tools are selected based on a risk

analysis conducted beforehand. The next step is the detection of incidents. Incident response team determines its scope and involves the appropriate parties. (Special Publication 800-61, 2012, p. 21) In the analysis stage, the response team defines affected networks and elements of the information system, causes and details of the incident. (Special Publication 800-61, 2012, p. 29) Followed by containment, the organization restrains the incident to minimize its effect on neighbouring IT resources or information system as a whole. (Special Publication 800-61, 2012, p. 21) In the stage of eradication and recovery, the incident response team eliminates compromised artefacts if necessary and restores the system to normal operations, possibly via reinstall or backup. (Special Publication 800-61, 2012, p. 37) Lastly, in post-incident activity, the organization documents details on the incident, retains collected data, and discusses lessons learnt. (Special Publication 800-61, 2012, p. 21)

2.4.4 Recovery objectives

Integration of recovery objectives into incident response plan determines an organization's incident response capability. Recovery objectives are of four types: recovery time objective (RTO), recovery point objective (RPO), service delivery objective (SDO), maximum tolerable outage (MTO). (Hotchkiss, 2010, pp. 10-11)

RTO is defined as the permissible time period for the recovery of a business process or function to its predefined operational levels after a disaster has taken place. Exceeding this time would pose a threat to the organization's survival or cause unacceptable losses. (Hotchkiss, 2010, p. 10)

RPO is a measure of the point to which data is to be restored. The reference point for the RPO is the point prior to the occurrence of the incident. Effective incident management and response can be achieved by closely linking RTO and RPO. (Hotchkiss, 2010, pp. 10-11)

SDO is defined as the degree of service that must be achieved within the recovery time period to bring it to acceptable levels. The acceptable level may be significantly less than the usual operation levels, less expensive, and easier to accomplish. (Hotchkiss, 2010, p. 10)

MTO is the time required for any process or function to operate at sustainable levels at a secondary or alternate site. The MTO value is arrived at by considering the types of events that may force operations to move to a secondary site and the estimated duration of such events. (Hotchkiss, 2010, p. 10)

2.4.5 Incident response capability assessment

There are two methods of identifying the current state of incident response capability in an organization. These are internal and external audits. (Apostol, 2014)

External audit is an assessment methodology that employs freelance, third-party auditors to sporadically review an organization's existing incident response capability. The external auditor uses in-reviews, surveys, simulations, and other assessment techniques to see the present capabilities and supply objective and impartial perspectives. An external audit is appropriate for a company that is trying to improve or re-engineer its existing incident management and response capability. (Apostol, 2014)

The incident management team performs a regular self-assessment exercise to identify the current state of incident response capability based on a set of predefined criteria. This exercise is easy to carry out because it does not require the involvement of all stakeholders. The self-assessment approach is preferred when companies want to quickly review their current response capability, without requiring the participation of several stakeholders. (Apostol, 2014)

2.4.6 Most common types of data leakage.

The report made by Info Watch Analytical Centre presents 10 most common incident types and respective safeguards. The report considers those data leakages which are caused by staff errors. (InfoWatch, pp. 8,9)

Table 2: Most common types of data leakage caused by staff errors (InfoWatch, pp. 8,9)

№	Incident	Safeguard
1.	Loss of an external storage devices	Staff training and awareness raising, encryption, monitoring of the devices and its content, data loss prevention software, destruction of the information, tag with an associated device number, tag with contact details of the owner
2.	Loss of mobile devices	Staff training and awareness raising, encryption, prohibition on storing information on devices, locks for laptops, mobile device tracking, remote destruction of the information, destruction of the information, tag with an associated device number
3.	Careless use of paper documents	Staff training and awareness raising, documents tagging, tag with contact details of the owner, printing controls
4.	Mistakes related to email sending	Staff training and awareness raising, data loss prevention software
5.	Mistakes related to mail and fax sending	Staff training and awareness raising

6.	Mistakes associated with access granting	Staff training and awareness raising, sophisticated access granting procedures and reviews, access granting controls
7.	Careless disposal of paper documents	Staff training and awareness raising, shredders, printing controls
8.	Careless disposal of equipment	Staff training and awareness raising, destruction of the information/equipment
9.	Disclosure during third party maintenance of equipment	Staff training and awareness raising, destruction of the information, non-disclosure agreements
10.	Social engineering	Staff training and awareness raising

3 Research and development methods

In this chapter, the methods and techniques are discussed used in the research and development. Various techniques are utilized in collecting, interpreting and analysing data. The third chapter explains the reasons why qualitative methods of research were used, what types of data collection were engaged, research process, development process, and ethical considerations.

3.1 Qualitative research methods

When conducting research, there are two different options on methods from which to choose. These are qualitative and quantitative research methods. Flick states that, “Qualitative research interested in analysing subjective meaning or the social production of issues, events, or practices by collecting non-standardised data and analysing texts and images rather than number and statistics.” (Flick, 2014, p. 542) Considering the research questions, the scope and the nature of the given thesis work, a qualitative research approach was applied to reach a desirable outcome. For the research to be able to get a better understanding of this thesis and to draw a conclusion, different methods were adopted during the research process. The thesis used qualitative research methods such as theoretical framework, thematic analysis, and case study including a semi-structured interview.

Utilizing case studies has many advantages, they provide data on real-life situations and provide better insight into the detailed behaviour of the topic of interest but are critical to not being able to generalize their findings (Yin, 2009, p. 18). Also, case studies are useful in research as researchers can examine gathered data on both small and large levels. There are many merits in using case studies as they contribute information on actual situations and give a more effective understanding to explore. (Kevin D, 2015, p. 81)

The case study of this work helped while carrying out research to carefully investigate information in a selected field. The process of the case study included linking thesis

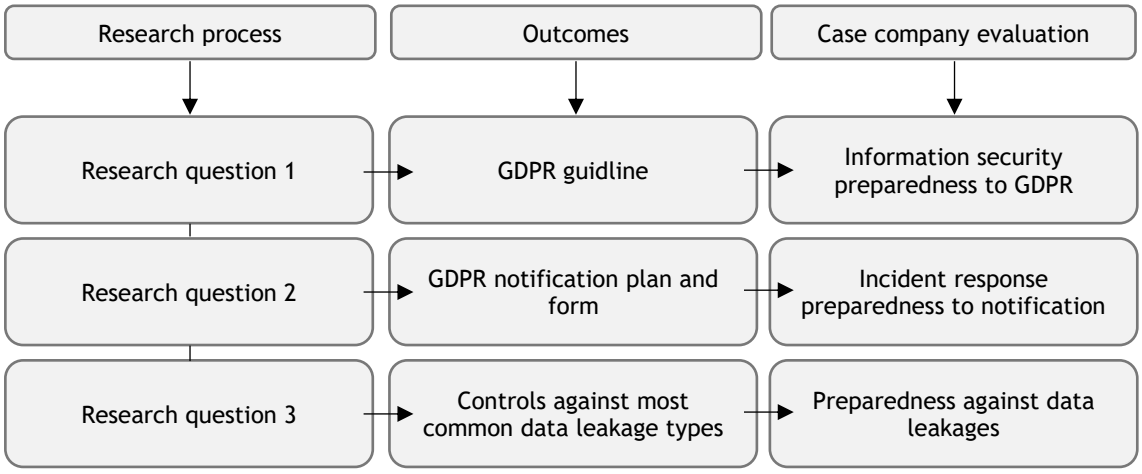


Figure 7: Thesis research process, outcomes, and case company evaluation linking

definitions with case company evaluation and a structure of the legal framework of the GDPR with corresponding findings of the case company evaluation. The relationship between research process, outcomes, and case company evaluation are shown in Figure 7.

3.2 Data collection

There are primary and secondary sources of data collection. (Kevin D, 2015, p. 77)

Primary sources are original data gathered on a specific topic for further studies. Primary sources give information from the first contact with the result of unprocessed information. It can be quantitative data (e.g. surveys, questionnaires) or qualitative (e.g. interviews, observations) data. (Kevin D, 2015, p. 77) In the main, there are unstructured, semi-structured, and structured interviews. Semi-structured interviews have advantages such as beforehand prepared questions addressing all the important issues, flexibility for interviewees in terms of language and views, and multiple interviewers can participate. (Kevin D, 2015, p. 119) A semi-structured interview can be used as one of the types of an interview for case study research. (Kevin D, 2015, p. 86) Thus, semi-structured interview (questionnaire Appendix 2) is chosen to gather original data from the case company and explained in paragraph 3.3.

Secondary sources are already existing data. This is the information that has been collected by others through primary sources. Secondary sources include published surveys and documents, published interviews and speeches, databases, archives, company reports, journal articles, and books. Theoretical background is also known as a secondary source as it provides information from previous researches. (Kevin D, 2015, p. 79) In the given work research process is based on the theoretical framework that includes regulations, company reports and guidelines, standards, and books. The research process is explained in detail in the next paragraph.

3.3 Research process

The given work uses a theoretical framework on which the works is based, and thematic analysis is applied further to answer the research questions of the thesis.

3.3.1 Theoretical framework method

Eisenhart defines theoretical framework as “a structure that guides research by relying on a formal theory; that is, the framework is constructed by using an established, coherent explanation of a certain phenomena and relationships”. (Eisenhart, 1991, p. 205)

Here are some of the advantages of employing theoretical framework method in a thesis. The theoretical framework method can be used as a guide to develop a study in terms of a research plan and data analysis, the method is helpful when determining appropriate

following research methods, examining theory can be easily structured, and it is easy to generalize the content of a study. (Eisenhart, 1991, p. 205)

To answer research questions of the thesis relevant literature is reviewed. These are the EC law in paragraph 2.1, compliance development theories in paragraph 2.2, information security and risk management (2.3) theories, and incident management (2.4) theories. The main documents of the theoretical framework are the GDPR, ISO/IEC 27005:2018 standard, NIST publications, and InfoWatch report on most common data leakage types. The theoretical framework reviews the requirements the GDPR poses before SME (research question 1), obligations of an organization to notify authorities communicating data breach (research question 2), and controls to mitigate the risks of most common data breach types (research question 3).

3.3.2 Thematic analysis method

One of the methods of analysing qualitative data is thematic analysis. (Kevin D, 2015, p. 140) Thematic analysis is “a method for identifying, analysing, and reporting patterns (themes) within data”. (Braun, 2006, p. 79)

In the given thesis work, first, thematic analysis was applied to the Regulation to highlight the main requirements of the legislation. The 7 principles of Article 5 and related articles were examined to reflect in the guideline (Appendix 1) statutory obligations for SMEs, NGOs and non-international organizations. Second, thematic analysis of Article 33 was conducted, where the main issues of notification process were defined in line with the incident management theories described in paragraph 2.4. Patterns of incident handling in conformity to the GDPR requirements were found. (See Appendix 3) And third, InfoWatch report (2.4.6) presents the most common data leakage types caused by staff errors. Analysing the frequency of mentioning and relevancy of information security controls against certain types of data leakages, relevant controls were identified in order of importance regarding organizational immunity from data leakage. (See Figure 8)

Thematic analysis of the GDPR resulted into the GDPR guideline (Appendix 1), analysis of the GDPR, ISO/IEC 27005:2018 information security standard, and NIST information security publications resulted in a notification plan and form (Appendix 3). Also, based on thematic analysis of InfoWatch report (2.4.6), risk assessment in ISO/IEC 27005:2018, and NIST Guide for Conducting Risk Assessments (2.3.3) relevant security controls, regarding most common data leakage types, are identified and reflected in a risk matrix in order of significance and risks associated with their absence in a security system of a company (see Figure 8).

3.4 Development process

Case company was interviewed and evaluated in the given work. Yin defines case study as “an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context”. (Yin, 2009, p. 18) The case company requested the thesis work to evaluate their preparedness to the GDPR, notification process to authorities, and most common data leakage types.

A questionnaire was created based on the research questions and its results (see Appendix 2). The questionnaire is divided into 3 parts of themes according to the three research questions and corresponding results. The interview questions are based on the guideline (Appendix 1), data breach notification plan and form, and risk matrix (Figure 8). Each question is related to each principle’s stipulation; the first part examines overall company compliancy level with the GDPR, the second part examines how well the company is prepared to data breach notification requirements, and the latter part examines the preparedness of the company to most common data leakage types. The given questionnaire was employed in a semi-structured interview to contribute to a broader understanding of the company preparedness and evaluation of the company afterwards. The interview was conducted with a case company representative.

The evaluation was completed after the semi-structured interview. Using thematic analysis, gaps were identified in information security of the case company concerning the compliance requirements of the GDPR, its data breach notification requirements, and data leakage controls. Risk matrix (see Figure 8) was used to assess the current risks in preparedness to most common data leakage types. Risk matrix includes the risks of data leakage and corresponding safeguards. The left column represents the safeguards in order of their importance in preventing those risks. The company’s information security risks of data leakage were evaluated based on the interview and reflected in the risk matrix, see Figure 8.

3.5 Ethical considerations

To make the given research and development work ethically mature, “Responsible conduct of research and procedures for handling allegations of misconduct in Finland” guideline of Finnish Advisory Board on Research Integrity (TENK) was reviewed. Principles of responsible research were followed. These are principles of integrity and accuracy of the research, proper methods of data gathering, respecting other researchers and publications, following standards, obtaining research consents and permits, and agreeing on rights and obligations. (TENK, 2012, p. 30)

During the research and case company evaluation, two interviews were conducted. The first interview was carried out with the information security professional to confirm the relevance of the theoretical framework and case company evaluation plan. The second interview was

conducted with the case company representative. Ethical aspects were considered in both interviews. Consents were obtained before the interviews, collected data remained confidential, and the identities of the participants were not disclosed.

Consent from the case company organization was obtained, meaning before conducting the research the objective of the research and the proposed length of the research were carefully discussed with the case company. The case company representative was aware of what data was being processed and the risks associated with the research. All collected data remained confidential.

4 Outcomes

This chapter delivers the results of the thesis and the case company evaluation. The GDPR guideline, GDPR data breach notification plan and form, and most important information security controls against data leakage caused by staff errors are described. Case company evaluation of overall GDPR compliance, preparedness to personal data breach notification, and preparedness to most common data leakage types are presented.

4.1 Guideline

The first research question regarding the requirements of the GDPR is answered. As a result, the thesis proposes a guideline based on the 7 principles of Article 5 and codes of conduct of the GDPR. The proposed guideline is suitable mostly to SME and NGO companies and does not cover the requirements for bigger companies or international corporations. The guideline can be found in Appendix 1 below.

4.2 GDPR data breach notification plan and form

The second research question is answered. Article 33 sets certain requirements for the procedure of notification of the authorities when a data breach occurs. Those requirements are reflected in the data breach notification plan and notification form. Also, information security risk management process of ISO/IEC 27005 standard (see Figure 3), data breach lifecycle of Fowler (see Figure 5), incident handling lifecycle of NIST (see Figure 6), and recovery objectives (2.4.4) are taken into account while building a personal data breach notification plan. GDPR data breach notification plan and notification form can be found in Appendix 3 below.

4.3 Controls to mitigate the risks of the most common data leakage types

The InfoSec report describes the most common data leakage types caused by staff errors and related safeguards. (See Table 2, subparagraph 2.4.6) Thematic analysis is used to analyse given data in the report and the following results are inferred. Security policies and staff training is the first control that should take place in a company. Secondly, monitoring tools for removable devices and access granting. Monitoring tools shall include DLP (for mobile devices and email sending), location tracking, and information filtering tools. Access granting processes should be monitored, analysed and changed periodically. Third, appropriate measures for data removal are required. This comprises information destruction tools for removable (mobile) devices, paper shredding, also tools for removal of data when equipment is given for maintenance or disposal. Next, encryption for removable and mobile equipment is important as well for protection against data leakage. Finally, item tagging is required for removable devices, mobile devices, and documents. The results were used further in the evaluation of the company preparedness to the most common data leakage types caused by

staff errors. Figure 8 shows the most important information security controls against data leakages caused by staff errors.

4.4 Information security preparedness and GDPR compliancy level at case company

The case company representative is aware of the main legal obligations and definitions. For example, the interviewee was aware of definitions such as personal data or consent, knew the requirements for data processing or notification period requirements. However, the main issue in the information security system of the case company is the limited introduction of security policies and training. GDPR certification from the relevant bodies was not obtained. Since it is a small-sized enterprise and has limited finances, it is not able to acquire certification according to an information security standard to ensure the CIA of data. Measures to ensure the CIA of personal data are implemented partially, which is described in paragraph 4.6.

To meet all the regulatory requirements of the law, the case company should first implement appropriate data protection policies and training on the GDPR. Second, information security controls to protect personal data (CIA triad), see paragraph 4.6. It would be advisable to get certified according to an approved information security standard. Also, the case company can obtain GDPR certification from approved bodies or follow an approved code of conduct if there is such in the industry.

4.5 Incident response preparedness to GDPR personal data breach notification

During the semi-structured interview, the company representative said that he was aware of the required notification time and knows contact details of the authorities. However, the interviewee did not know all the particularities of the requirements of notification such as requirements for the description of the possible impact of a personal data breach and description of actions taken for risks mitigation. There was no notification plan, notification template, and a ready-to-use list of contacts of persons whom to notify about a data breach.

This work proposes a GDPR personal data breach notification plan and form that can be used by the case company. The notification plan and form include all the requirements of the Regulation to the notification process. These documents can be found in the attachment as Appendix 3.

4.6 Preparedness of case company to most common data leakage types

The company's information security risks were evaluated based on the interview and responses of a company representative. The results are reflected in the risk matrix (see Figure 8). The risk matrix is built based on risk assessment (see Figure 4) and thematic analysis results (see paragraph 4.3) The formula used is $[Risk\ level] = [Security\ measures\ and\ related\ risks] \times [Preparedness]$

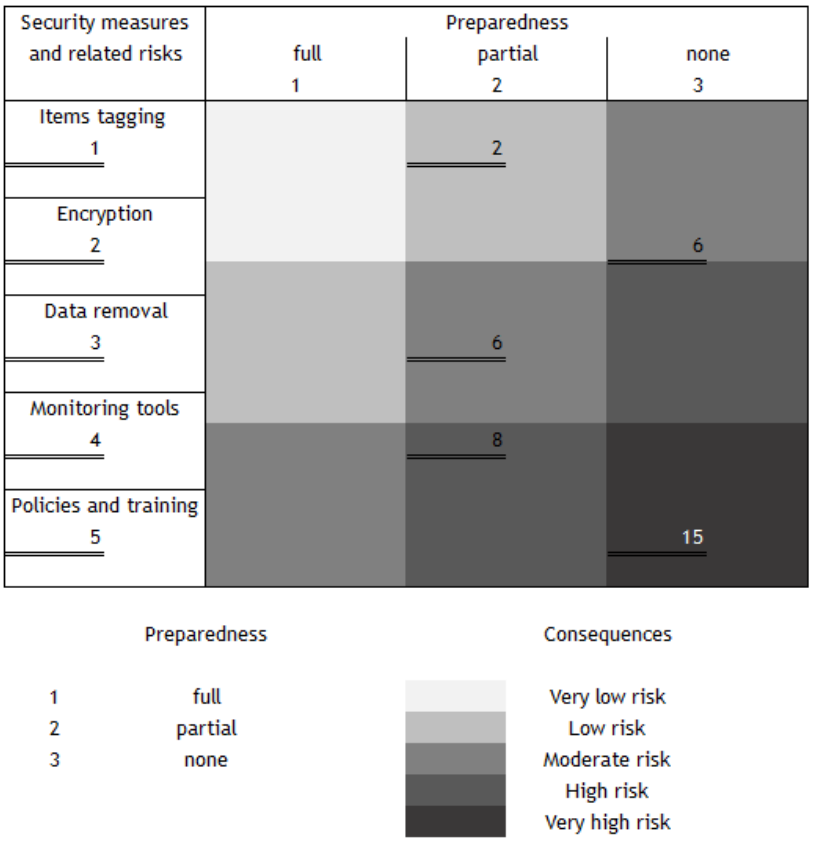


Figure 8: Case company risk matrix for most common data leakage types caused by staff errors and related security measures

Information security policies and training are introduced to a very limited extent, this imposes very high risks on the operations of the company. The case company introduced only some monitoring security measures, which results in high risks. Missing encryption and partially implemented data removal measures are associated with moderate risks, partial implementation of items tagging is associated with low risks. Based on the risks matrix, the most important measure to be taken into consideration for further development by the company is policies and training; second, monitoring tools, third, data removal, and encryption; lastly, items tagging.

4.7 Compliance culture at case company

The interview and evaluation of the case company resulted in a clear vision of the overall compliance culture. The case company shows a willingness to comply with the Regulation and involves basic frameworks in its information security system. According to Table 1 “Levels of corporate maturity” of Jackman, the compliance state of the case company meets the levels between minimum standards and compliance culture, levels 2 and 3 respectively. The culture of the company can be characterized by an unwillingness to make decisions, ill-conceived compliance, and no proactive steps taken. The compliance can be described as such that

there is a weak level of governance and superficial personal data protection policies in the information security system of the organization.

To improve compliance performance the case company may introduce and practice the mechanisms mentioned in paragraph 4.4. These are personal data protection policies, GDPR code of conduct, or GDPR certification.

5 Conclusion

This work describes the Regulation from the compliancy development perspective, how a company can be compliant based on the law. Compliance of a company with the Regulation is dependent on adherence to the principles described in Article 5. It is important to note that level of imposing fines is based on such factors as premeditation of the GDPR violation, measures taken to mitigate the risks, notification particularities (Article 33), recitals (148) and (150). (European Union, 2016) Presence of personal data protection policies, information security policies, adherence to codes of conduct, personal data breach notification plan, and security standards can help significantly to avoid fines or lower the levels of fines in case of law infringement.

The given thesis looked for answers to questions related to various compliance areas such as information security and incident response. The first part of the thesis explored the sensitive areas in the GDPR legislation, while the second part focused on the theories of information security, risk management with controls within information security. After the background was explored it was necessary for the case company to know the relevant factors when responding to a data breach incident. Therefore, lastly, the thesis explored the methods and processes of incident management.

The process of handling private data can be divided into three stages. First, data subjects give consents when a controller is processing their private data. Second, the processed data may be categorized into confidential and personal data which require the involvement of special security measures to protect the data. Finally, implementation of information security controls and GDPR compliance techniques are necessary to protect personal data and related company’s processes. GDPR guideline (Appendix 1) defines what is personal data and legal bases for the processing of a data subject's personal data. Information security controls (Figure 8) allow a company to handle personal data securely, especially to ensure authorized access to personal data.

The problem of many SMEs is that incidents of data breaches remain undetected due to the fact that breach detection systems of the organizations are underdeveloped. According to the Regulation's requirements regarding notification of the authorities on data breaches, it is crucial for a company to be able to identify what type of a breach has occurred and determine the impact of the given data breach. It is important to note from a perspective of cybersecurity, that between the periods of identification of data breach type and impact assessment, elimination of causes of information security breaches and fortification of weak zones are necessary to be undertaken. According to the GDPR, once a company has suffered a data breach, it has 72 hours to report incident details to the authorities. All the collected information should include information on how a data breach has occurred, what and when did it occur, who was involved, why it occurred and what is the impact of the given data

breach. Abidance to these requirements of the GDPR can help decrease the fines in case of violation of the law. It is worth noting, that a company should identify the sources of a data breach, whether it was of an internal or external origin. This information can help to conduct forensic analysis and help during the following investigations. For the most part, breaches caused by internal sources, it is for that reason the given work defined information security controls against most common data leakage types caused by staff errors. (See Figure 8) These controls include policies and training, monitoring tools, data removal, encryption, and items tagging.

The case company agreed on the benefits of putting information security and incident management tools in place according to the GDPR guideline (Appendix 1) and GDPR personal data breach notification plan and form (Appendix 3). It will bring benefits to the organization in terms of developing managerial skills and staying up to date with what might be a threat to the organization. Building a compliance-minded culture can forestall law violations and data leakages, it is inseparable from the image of the company, and plays a great part in forming the company's credibility.

5.1 Review of the results

Focusing on SMEs and based on Article 5 of the GDPR, all the requirements of the legislation were investigated. The requirements of the Regulation are reflected in the guideline (Appendix 1), in personal data breach notification plan and form (Appendix 3); also, the main safeguards to most common data leakage types caused by staff errors were found (Figure 8). The guideline includes essential features of the law to help an SME become compliant with the Regulation. Additionally, code of conduct is included in the guideline, which can be implemented into the policies and processes of a company.

The case company interview and evaluation showed that the company was familiar only with some of the legal requirements. However, it is not enough to prove the willingness of the company culture to be compliant with the Regulation. It is important to change the integral culture of the company, where its information security culture is only in its infancy. There were no information security policies and no relevant certifications were acquired. The company shall show adherence to codes of conduct, obtain a certification from a relevant body, and introduce a proper personal data breach response mechanism to inform authorities in case of the GDPR violation. These steps towards compliancy with can help either deter a possibility of the Regulation infringement or at least soften the severity of the penalties incurred in case of an infringement. In addition, the case company can protect personal data of data subjects with the help of information security controls mentioned in paragraph 4.6.

5.2 Discussion of the results

This work focused on the Regulation requirements and compliance development from the standpoint of information security management. The research results of the given work can be used by SMEs and information security officers to prepare SMEs to the GDPR, personal data breach notification procedures, and to become familiar with relevant information security controls against data leakages caused by staff errors. Further studies on the topic of GDPR compliance can examine the legislation from a perspective of cybersecurity, CIA triad, and the technical aspects of information security. Also, the given work covered SMEs excluding NGOs and non-international companies. Likewise, further studies can conduct research on compliance of international organizations or NGOs.

As a result, all three research questions were answered. The outcomes of the thesis are the GDPR guideline, data breach notification plan and form, risk matrix of the most common data leakage types caused by staff errors and its corresponding information security controls. Respectively to the research questions, evaluation of the company was carried out successfully with the approval of the case company. The case company shows a willingness to comply with the GDPR and is implementing security measures according to the evaluation.

References

Printed sources

Babbie, E. R. 2010. The practice of social research (Vol. 12). Belmont, CA : Wadsworth ; London : Wadsworth Cengage.

Braun, V. 2006. Using thematic analysis in psychology. Qualitative Research in Psychology , 77-101.

Eisenhart, M. 1991. Conceptual Frameworks for Research Circa 1991: Ideas from a Cultural Anthropologist; Implications for Mathematics Education Researchers. (pp. 202-219). Blacksburg.

Flick, U. 2014. An introduction to qualitative research (5th ed.). London: Sage Publications Ltd.

Friedland, M. (Ed.). 1989. Sanctions and Rewards in the Legal System : A Multidisciplinary Approach. Canada: Toronto Press.

Friedland, M. (Ed.). 1990. Securing Compliance : Seven Case Studies. Canada: University of Toronto Press.

Hotchkiss, S. 2010. Business Continuity Management : In Practice. In S. Hotchkiss. BCS Learning & Development Limited.

ISO/IEC 27005. 2018. Information technology. Security techniques. Information security risk management.

Jackman, D. 2015. The Compliance Revolution : How Compliance Needs to Change to Survive. Singapore: John Wiley & Sons, Incorporated.

Johnson, M. K. 2014. Computer Incident Response and Forensics Team Management. Syngress.

Kevin D, P. O. 2015. Research Methods for Business and Management : a guide to writing your dissertation. Goodfellow Publishers Ltd.

Strauss, J. C. 2008. Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory. California: Sage Publications.

Taylor, A. 2013. Information Security Management Principles. In A. F. David Alexander, & A. Taylor (Ed.), Information Security Management Principles (2nd ed., pp. 26-28). BCS Learning & Development Limited.

TENK. 2012. Responsible conduct of research and procedures for handling allegations of misconduct in Finland.

Yin, R. K. 2009. Case Study Research: Design and methods. London: Sage.

Electronic sources

Apostol, A. 2014. Cyber Essentials – Internal and External Security Assessments Explained. Accessed 20 December 2018. https://www.itgovernance.co.uk/blog/cyber-essentials-internal-and-external-security-assessments-explained

Baskerville, R. 2014. Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management, 51(1), 138-151.

Accessed 27 September 2018. https://www.sciencedirect.com/science/article/pii/S0378720613001171

English Oxford Living Dictionaries. No date. English Oxford Living Dictionaries. Accessed 01 February 2019. https://en.oxforddictionaries.com/definition/compliance

European Union. 1995. eur-lex.europa.eu. Accessed 27 September 2018. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Union. 2012. Chapter of fundamental rights of the European Union. Accessed 27 September 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

European Union. 2016. Accessed 27 September 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Federal Information Security Modernization Act of 2014. 2014. Accessed 27 September 2018. https://www.congress.gov/bill/113th-congress/senate-bill/2521/text

Fowler, K. 2016. Data Breach Prepararion and Response, Breaches are Certain, Impact is Not. Cambridge: Syngress. Accessed 30 September 2018. http://ebookcentral.proquest.com/lib/laurea/detail.action?docID=4556899

Jajodia, S. 1999. Trusted recovery, association for computing machinery. Communications of the ACM, 71-75. Accessed 27 September 2018. https://dl.acm.org/citation.cfm?id=306549.306580&coll=portal&dl=ACM&preflayout=flat#prox

Jouinia, M. 2014. Classification of security threats in information systems. Procedia Computer Science. Accessed 11 February 2019. https://ac.els-cdn.com/S1877050914006528/1-s2.0-S1877050914006528-main.pdf?_tid=ea539695-fbd3-46ab-91b2-286524a5c98e&acdnat=1551081535_f459839a1a7a300226ef2dd48ccf1844

IAPP. No date. IAPP. Accessed 31 January 2019. https://iapp.org/media/pdf/resource_center/Categories-of-personal-information.pdf

InfoWatch. No date. 10 Most Widespread Staff Errors behind Data Leakage. Moscow: InfoWatch Analytical Center. Accessed 12 February 2019. https://infowatch.com/sites/default/files/private_files/557987362c1ab_eng.pdf

ISACA. 2012. Incident Management and Response. Accessed 12 February 2019. http://www.isaca.org/Knowledge-Center/Research/Documents/Incident-Management-and-Response_whp_Eng_0312.pdf

Stewart, J. 2012. CISSP: Certified Information Systems Security Professional Study Guide. John Wiley & Sons, Incorporated. Accessed 12 February 2019. http://ebookcentral.proquest.com/lib/laurea/detail.action?docID=875861

Kendall, K. 2005. Understanding Disaster Recovery Planning through a Theatre Metaphor: Rehearsing for a Show that Might Never Open. Communications of the Association for Information Systems, 1001-1012. Accessed 27 September 2018. https://aisel.aisnet.org/cais/vol16/iss1/54/

NIST. 2002. Risk Management Guide for Information Technology Systems. Accessed 11 February 2019. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

NIST Special Publication 800-30. 2012. Guide for Conducting Risk Assessments. Accessed 03 March 2019. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

NIST Special Publication 800-61. 2012. Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology. Accessed 27 September 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NISTIR 7298. 2013. NISTIR 7298, Glossary of Key Information Security Terms. Accessed 04 March 2019. https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Probst, C. 2010. Insider Threats in Cyber Security. Boston: Springer. Accessed 11 February 2019. https://link.springer.com/book/10.1007/978-1-4419-7133-3

Figures

Tables

Appendices

Appendix 1: First appendix

GDPR guideline

Main Terms

"'**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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", Article 4 (1);

"'**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", Article 4 (2);

"'**pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person", Article 4 (5);

"'**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", Article 4 (7);

"'**processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller", Article 4 (8);

"'**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", Article 4 (11);

"'**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" Article 4 (12);

"'**supervisory authority'** means an independent public authority which is established by a Member State pursuant to Article 51", Article 4 (21);

"'**international organisation'** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries", Article 4 (26).

[Article 4] (European Union, 2016)

Main principles

The EU law of GDPR is of big proportions and may overwhelm your company with its requirements to personal data processing. However, the regulation can be broken down into the units. This can help organizations to understand basic concepts of the law and start preparing for the Regulation. The fundamental article of the law is Article 5: "Principles relating to processing of personal data". 7 main principles of Article 5 constitute the whole regulation. These principles are “Lawfulness, fairness and transparency”, “Purpose limitation", “Data minimization”, “Accuracy”, “Storage limitation”, “Integrity and confidentiality”, and “Accountability”.

N	Principle	Description	Related articles
1	Lawfulness, fairness and transparency	Keep the data processing legal and fair; state what your company is going to do with the data in clear terms.	Article 6 “Lawfulness of processing”, Article 9 “Processing of special categories of personal data”, Article 89 (1) “Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes”
2	Purpose limitation	Do not do more with the data than it is stated in a consent your company would do.	Article 6, Article 13 “Information to be provided where personal data are collected from the data subject”, Article 26 “Joint controllers”
3	Data minimization	Do not collect more data than your company needs.	Article 25 “Data protection by design and by default”
4	Accuracy	Keep personal data up to date and deal with inaccuracies as soon as possible.	Article 16 “Right to rectification”, Article 17 “Right to erasure (‘right to be forgotten’)”, Article 18 “Right to restriction of processing”
5	Storage limitation	Do not keep the processed data for a longer period of time than it is necessary.	Article 6, Article 17, Article 89 (1)
6	Integrity and confidentiality	Keep the personal data safe while your company deals with it.	Article 24 “Responsibility of the controller”, Article 25, Article 32 “Security of processing”
7	Accountability	Be able to show that your company complies with the above GDPR principles.	Article 24, Article 25, Article 83 “General conditions for imposing administrative fines”

[Article 5, Article 6, Article 9, Article 89 (1), Article 13, Article 16, Article 17, Article 18, Article 24, Article 25, Article 26, Article 32, Article 83, Article 89 (1)] (European Union, 2016)

Principle 1 - Lawfulness, fairness and transparency

Processing of personal data is to be lawful, it must meet at least one of a number of, and an important first step in considering your organization processing activities is to clearly establish which of the criteria applies in any given situation.

N	Lawfulness, fairness and transparency aspects
1	The data subject has consented to data processing.
2	There is a need to perform a contract between your organization and the data subject, or to see whether a contract can happen.
3	Your organization legally must do data processing.
4	Your organization protects the vital interests of the data subject.
5	Personal data processing in the public interest.
6	It is for legitimate interests of the company, as long as it does not affect the data subject's rights and freedoms.
7	Consent for processing personal data from a data subject should be obtained in a clear and simple form

Controllers and processors are prohibited to process special categories of data ("sensitive data") such as data related to the origin, political opinions, beliefs, trade union membership, genetics, biometrics, health, and sex life. An exception is applied when a data subject has given a consent for specified purposes.

[Article 5, Article 6, Article 9] (European Union, 2016)

Principle 2 - Purpose limitation

Data processor shall use the information gathered from a natural person only for the purposes agreed between them. Your company is to be clear with a data subject from the beginning of data processing on the reasons for data collection

N	Purpose limitation aspects
1	Process personal data only for specified purposes
2	Use joint controller agreement in case your company is going to share personal data with other companies. Define the purposes and methods joint controller is going to use while data processing.

In the event that a joint controller has been organized, roles and responsibilities among controllers in relation to the data subject should be agreed among the members. The data subject should be informed that a joint controller has been arranged. Also, you need to remember that all the rights remain valid in regard to each of the participants of the joint controller.

[Article 5, Article 13, Article 26] (European Union, 2016)

Principle 3 - Data minimization

Data minimization means that your company cannot collect more data than it needs. Limited and relevant according to its usage purposes, and accurate information of data subjects is to be processed by your company.

N	Data minimization aspects
1	Employ technical and organizational safeguards through all the business processes for data minimization, “data protection by design and by default” concept.
2	Collect and store only purpose specific personal data.

[Article 5, Article 25] (European Union, 2016)

Principle 4 - Accuracy

Your company should keep personal data up to date and deal with inaccuracies as soon as possible. Your company should be aware of the data subject rights of personal data rectification and erasure.

N	Accuracy aspects
1	Amend incorrect personal data and remove personal data that is no more needed for the purposes of the organization without undue delay.
2	Ensure data subject has rights to rectify processed personal data in case of its inaccuracy within the proper time period.

[Article 5, Article 16, Article 17, Article 18] (European Union, 2016)

Principle 5 - Storage limitation

GDPR requires your organization to remove personal data if there is no longer a need for this information in relation to the purposes of use stated by the company. Keep in mind GDPR stipulation about personal data erasure, which is known as 'the right to be forgotten'. A natural person has the right to ask your company to erase his/her personal data from your records.

N	Storage limitation aspects
1	Your organization shall store personal information only for a period when the data is needed.
2	Employ appropriate procedures in order to act in accordance with GDPR stipulation about personal data erasure right of an individual.

Your organization can store personal data if it has been gathered on scientific, historical, statistical purposes or on purpose in the interest of the public. In this case, for compliance, your organization needs to employ corresponding organizational and technical measures, for example, it can be data pseudonymization in respect to data minimization. This would make impossible further identification of data subjects.

[Article 5, Article 6, Article 17, Article 89(1)] (European Union, 2016)

Principle 6 - Integrity and confidentiality

Your organization must keep the processed data safe. All the operations of data processing and storage processes must be protected with appropriate technical and organizational safeguards.

N	Integrity and confidentiality aspects
1	Apply proper measures depending on the risks of unauthorized access to ensure safe processing and storage of personal data.
2	Ensure that your company has developed data protection policies.
3	Make sure you have taken appropriate measures to implement 'confidentiality, integrity, availability' concept into the processes and services of your organization.
4	It is advisable to introduce the pseudonymisation and encryption of personal data into the information systems of your company.
5	You have to be able to restore access to personal data in case if a security incident has happened.
6	Make sure that company employees process personal data based on data processing instructions.

[Article 5, Article 32] (European Union, 2016)

Principle 7 - Accountability

Your organization must be able to show that it complies with the 6 principles of the GDPR listed above. Here is an overall view of holistic approaches to be GDPR compliant with its stipulations.

N	Accountability aspects
1	Apply measures to be compliant with 6 principles mentioned above employing appropriate organizational and technical safeguards.
2	Apply code of conduct and obtain certification from the supervisory authority.
3	Implement data protection policies.

It is important to remember the "Data protection by design and by default" concept, which according to GDPR requires companies to embed protective measures into the company processes and services.

[Article 5, Article 24, Article 25] (European Union, 2016)

Code of conduct

The regulation makes provision for member states and industry bodies to create codes of conduct and certification schemes that can be used to encourage companies to demonstrate compliance. It is well worth keeping eye on what is happening in your industry and country. Your organization can apply a code of conduct with different requirements depending upon the sizes of the organization. There are possible topics in the following table which such code of conduct can cover.

N	Code of conduct aspects approaching GDPR
1	Fairness and transparency of data processing
2	Legitimacy of data processing
3	Process of collection of personal data
4	Pseudonymization of personal data when it is required
5	Information provision to the public or a data subject
6	Abidance by the rights of data subjects
7	Protection for children and parental responsibility regarding personal data processing
8	Security of processing of personal data
9	Personal data breach notification to authorities and individuals
10	Transfer of personal data to international organizations or third countries
11	Nonjudicial procedures for resolving data processing disputes between controllers and data subjects

If your company abides by the code of conduct set by a relevant entity it can grant you a certification of compliance with GDPR.

[Article 40, Article 42] (European Union, 2016)

Appendix 2: Questionnaire for semi-structured interview

GDPR compliance at case company, questions according to the guideline of Appendix 1

1) What is your organization definition for personal data? What type of personal data does your company hold?

   Lawfulness, fairness and transparency principle

2) If your company processes personal data, do you ask consent for processing data from a data subject?

3) Are the consents and agreements for processing data freely given and unambiguous?

   Purpose limitation principle

4) What are the purposes your organization processes personal data?

5) Does your organization share personal data with third parties? If yes, does your organization define the purpose and methods of data processing?

   Data minimization principle

6) Do you process and store only relevant information to the purposes of processing?

   Accuracy principle

7) Do you remove or update personal data which is inaccurate?

8) How have you ensured the data subject's right to rectify and erase personal data?

   Storage limitation principle

9) For how long do you store personal data? How have you ensured that your organization does not keep personal data for a longer period than it is needed?

10) Have you ensured procedures for personal data erasure right for natural persons?

    Integrity and confidentiality principle

11) What security measures do you have in place to protect the processing and storage of personal data from unauthorized access?

12) Does your organization have data protection policies?

13) How does your organization ensure information security? Does it follow any security standards?

14) Do you use encryption at your company?

15) How have you ensured the possibility of the restoration of access to personal data after a data breach?

16) Does your company have instructions for the staff on how to process personal data?

Accountability principle

17) Which organizational and technical tools do you apply to be compliant with the above-mentioned principles?

18) Have you acquired any certification from supervisory authority? Do you follow a code of conduct, if there is any?

GDPR data breach notification process

19) Do you have a GDPR data breach notification plan?

20) Do you know the main requirements for data breach notification process?

    a. What is the required time period of notification of the authorities?

    b. Do you know which authorities you shall contact?

    c. Do you have a ready-to-use list of contacts that you need to notify?

21) Do you know what details about personal data breach your company needs to report to the authorities?

22) Do you have a notification template, and do you know what details of data breach you must communicate to the authorities?

23) Do you have partners with whom you share personal data? Have you agreed with your partners on how to communicate in case of a data breach?

Preparedness to most common data leakage types

24) Do you have information security policies and staff training at your company?

□ Full □ Partially □ None

25) Do you apply monitoring tools such as data loss prevention and access granting software? (Monitoring of the content of the devices)

□ Full □ Partially □ None

26) Do you destroy sensitive (such as personal data) information when it is no longer in use? (Storage devices, mobile devices, paper shredding, equipment disposal, outsourced equipment maintenance, remote wipe)

□ Full □ Partially □ None

27) Do you encrypt data? (In general, and particularly, external devices and mobile devices)

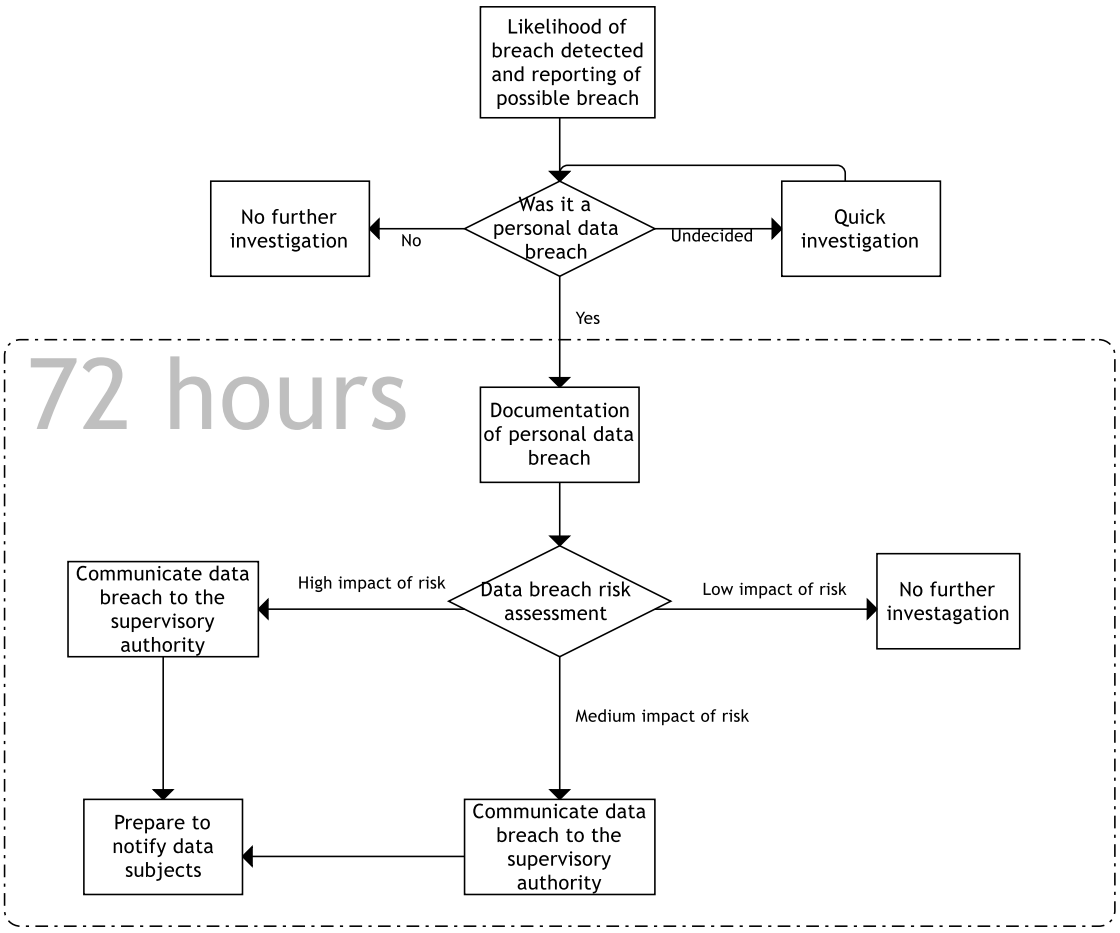
□ Full □ Partially □ None

28) Do you mark documents and tag company items? Do you keep a register of devices, documents, and other items?

□ Full □ Partially □ None

Appendix 3: GDPR personal data breach notification plan and form

Personal data breach notification plan



Personal data breach notification form

Contact name:	
Title:	
Organization name:	
Contact address:	
Contact phone number:	
Contact email address:	
Date and time of notification submitted:	
Date and time of detection of breach:	
Period between detection and notification:	

Personal data breach description
E.g. Classification (customers, employees, subscribers, and so on) and the number of data subject affected. Classification (names, addresses, bank account numbers, and so on) and the number of personal data affected. Describe the current knowledge of data breach accident. External or internal cause. Is it lost or stolen device, lost or stolen paper, hacking, wrong address emailing, and so on.

Impact of data breach
E.g. Description of the likely risks data subjects might face and consequences of the personal date breach.

Actions taken to mitigate risks and unfavourable effects
E.g. Description of the actions that have been taken before the notification process to reduce the negative impact of the breach, stop any future breaches and reduce risks to data subjects.

Proposed actions to mitigate risks and unfavourable effects
E.g. Describe the further actions that presumed to be taken to reduce and stop the adverse impact of the breach.

Possible delay of notification
E.g. If the 72 hours timeframe required for the notification has not been met, the reasons for the delay should be stated.