GDPR compliance guidebook for employees at a single University of Applied Sciences in Southern Finland

Elizabeth Hohtar

2019 Laurea

Laurea University of Applied Sciences

GDPR compliance guidebook for employees at a single University of Applied Sciences in Southern Finland

Elizabeth Hohtar
Security Management
Bachelor's Thesis
March, 2019

Laurea University of Applied Sciences
Safety, Security and Risk Management

Abstract

Hohtar, Elizabeth

GDPR compliance guidebook for employees at a single University of Applied Sciences in Southern Finland

Year 2019 Pages 57

The purpose of this thesis project is to produce the guidebook under the name "GDPR compliance guidebook for employees at a single University of Applied Sciences in Southern Finland", which was commissioned by Laurea University of Applied Sciences. The objectives are to follow the requirements of the project's client and workplace supervisor Tiina Ranta, produce an informative and useful guidebook and study the appropriate legislation such as General Data Protection Regulation. The guidebook was created in response to high risks in data protection with the purpose to lower these risks.

The "GDPR compliance guidebook for employees at a single University of Applied Sciences in Southern Finland" was based on the risk assessment summary created by Tiina Ranta, the Head of Security at Laurea University of Applied Sciences. The literature review was conducted in order to study the General Data Protection Regulation that was enforced in May 2018.

The methods included planning and organizing the text layout of the guidebook as well as following the requirements from the thesis project's client. The material was collected and analysed for further use in the guidebook. The meetings with the client and data protection officer helped to establish specifications for the guidebook. Furthermore, the advice and feedback from the client and data protection officer helped to improve the structure of the guidebook.

The result of the thesis project is the structured text for the GDPR compliance guidebook. The produced guidebook met all requirements with satisfaction. The guidebook contains 4 short sections based on general risk assessment summary. Each section contains legislation, which is the General Data Protection Regulation with the addition of the Universities of Applied Sciences Act. The sections of the guidebook include real-life case examples, recommendations, and questions, which are meant to trigger a discussion and critical thinking analysis.

In conclusion, recommendations include improving guidebook in the future by adding new cases and new knowledge on General Data Protection Regulation, creating an electronic interactive version of the guidebook to engage more people and producing a GDPR-related webpage on Laurea University of Applied Sciences website for everyone to be aware of their data protection rights.

Keywords: General Data Protection Regulation, Guidebook, Guidelines for employees

Table of Contents

1 Introduction

Privacy is a fundamental human right in the European Union. In order to understand the importance of data privacy and data protection, it's important to remember the socio-political history of the EU and the historical events that led to how data protection is treated today. The fascist regimes such as Hitler's Gestapo in Germany, Stalin's KGB (or Committee for State Security) in USSR, Honecker's Stasi (The Ministry for State Security or State Security Service) in East Germany, Salazar's PVDE (The State Surveillance and Défense Police) in Portugal and Franco's Secret Police in Spain, all these regimes were built on violating the privacy of natural persons, being able to access personal and sensitive information and therefore, control the population. (Bermann, S. Grimm, D. Zanfir-Fortuna, G., 2018)

In 1948, the United Nations General Assembly pronounced in the Declaration of Human Rights, Art 12, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (United Nations, 1948)

In 1995, the Directive 95/46/EC of the European Parliament on the protection of individuals with regard to the processing of personal data (Art. 1.1), stated "In accordance with this Directive Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their rights to privacy with respect to the processing of personal data." (European Union, 1995)

In May 2018, the GDPR was enforced replacing the Directive 95/46/EC. Considering historical events, the importance of data protection of European citizens is evident. For non-compliance with GDPR, the fine would be 4% of the total revenue or 20 million, depending on what is higher. (GDPR, Chapter 8, Art. 83) Which is why it is important to be prepared for the proper understanding of GDPR compliance. Therefore, creating the GDPR compliance guidebook for employees was meant to raise awareness regarding handling sensitive information in order to avoid a data breach. GDPR compliance among the UAS employees will not only decrease the data protection risks but also careful handling of sensitive information will solidify the integrity of the University of Applied Sciences.

This thesis project was requested by Laurea University of Applied Sciences (UAS). The aim of the thesis project was to produce The General Data Protection Regulation guidebook to ensure GDPR compliance among the employees of UAS. The guidebook will be distributed among the employees of UAS in order to serve a practical use.

This thesis report includes a literature review on earlier research and discussions concerning the General Data Protection Regulation, which was conducted in order to investigate the current state of GDPR in higher educations in Europe as well as in the United States of America. The theoretical framework presents legislation used for the creation of GDPR compliance guidebook. The requirements set by this project's client for the guidebook and its structure are expanded on in the methodology chapter as well as the methods used during the work on the guidebook. To conclude this thesis report, practical uses of the guidebook are discussed as well as feedback from the client along with the recommendations on what could be done to improve the handling of personal information. The final text for the "GDPR compliance guidebook" is presented in appendices.

2 The purpose of the Thesis project.

The purpose of this thesis project for Universities of Applied Sciences is to reduce data protection risks.

The University of Applied Sciences requested this thesis project to reduce high data protection risks the UAS network was facing. One of the options for treating these risks was the creation of the guidebook. "GDPR compliance guidebook for employees" was built around the highest risks from risk assessment conducted in UAS, and the material in the guidebook was meant to raise awareness, give basic information on GDPR and help the employees with an understanding of how to avoid privacy and data breaches.

The following risk assessment summary was provided by the thesis project supervisor Tiina Ranta. These risks are typical for educational institutions in general, but they are not specific to any UAS in particular.

There are no guidelines for handling sensitive information. The staff does not understand how to deal with sensitive information - electronic, verbal, manual data processing. Public spaces are typical places where people share (loudly) sensitive issues with each other. Sensitive information can be leaked because the recipient's legitimacy to the data is not checked. Sensitive information is dealt with in systems where it should not be done. The backgrounds of staff members are not checked. Outside parties do not adequately protect the information. Unnecessary documents will not be destroyed immediately. (Risk Assessment summary for UAS 2018)

2.1 Limitations

The main limitation of this thesis project would be the novelty of the General Data Protection Regulation, which was only enforced in May 2018. The lack of experience with GDPR, in general, limits the research of available information and examples of GDPR-related cases, needed for

this project. At this point, not many GDPR sources are available to learn from, because, many professionals are currently studying the regulation and getting familiar with it.

After researching the material and analysing the literature review it became clear that for this thesis project interviewing UAS employees will not yield results since the GDPR implementation is at its early stage.

In practice, there weren't many cases of GDPR enforcement and in the higher education field discussion, some universities in the USA don't think that GDPR will work effectively. However, it is a good opportunity to contribute to the GDPR understanding at the very beginning, and then assume that with more time and with more information available the guidebooks can be improved by other students or professionals in the future

The challenging part of the project was to come up with real-life examples of data breach set in universities, based on specific risks and then build the recommendations on it. The limitation consisted of three parts. First was the fact that newspaper articles were limited to these in the English language, therefore some of the local news articles were not available for the research. The second difficulty was that the newspaper articles mostly discuss data breaches happened in big corporations, rather than universities. Another important obstacle was that these examples were described in a general way without going into many details, which is an understandable security measure, but it made these cases hard to categorise and fit into appropriate sections. All these limitations led to the changes in guidebook structure. For example, instead of real-life cases set in universities, it was decided to concentrate on what was available for the analysis.

2.2 Development Project

The form of the bachelor's thesis "GDPR compliance guidebook for employees at a single University of Applied Sciences in Southern Finland" would qualify as a development project. The task is to develop and structure the text for a guidebook. The guidebook will raise awareness among the employees regarding the handling of personal and sensitive information, which as a result will reduce data protection risks in UAS, as Figure 1 (GDPR compliance guidebook process) illustrates this three-step process to better understand the purpose of the development task.

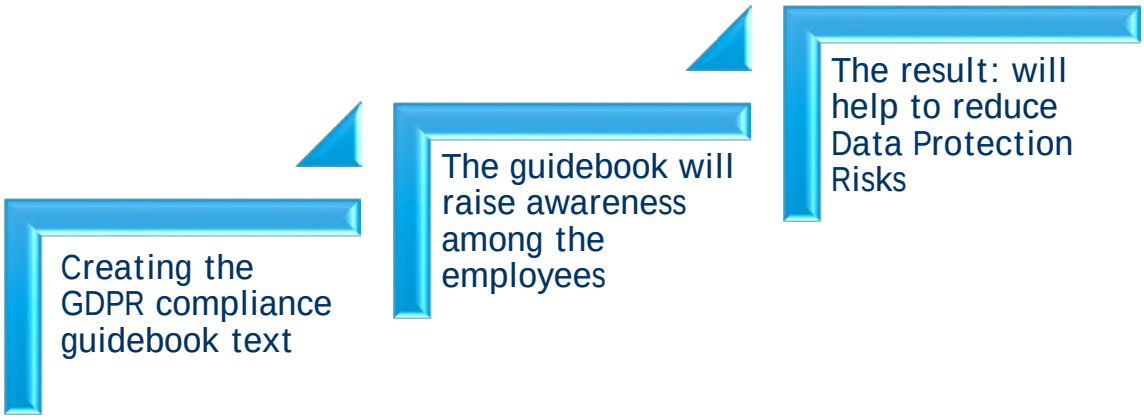

Figure 1: GDPR compliance guidebook process

The GDPR compliance guidebook for employees is meant to carry out a practical purpose by raising data protection awareness among the employees of UAS. The guidebook will be based on the General Risk Assessment Summary (2018, Ranta) for the single University of Applied Sciences in Southern Finland, but it can be used in multiple other Universities of Applied Sciences to help guide their employees through the risks of GDPR compliance and similarly reduce data protection risks.

Theoretically, this development project can serve an educational purpose as well, for those who would like to expand their knowledge on the subject.

In order to complete the development task, the research should be conducted first, as Figure 2 (Steps of Thesis Project) illustrates. The aim of the research is to learn about GDPR in higher education facilities. The research question is “How do other universities implement the GDPR?". In this thesis project, the research is conducted in the form of a literature review under the name of "Earlier research and professional discussion in the field".

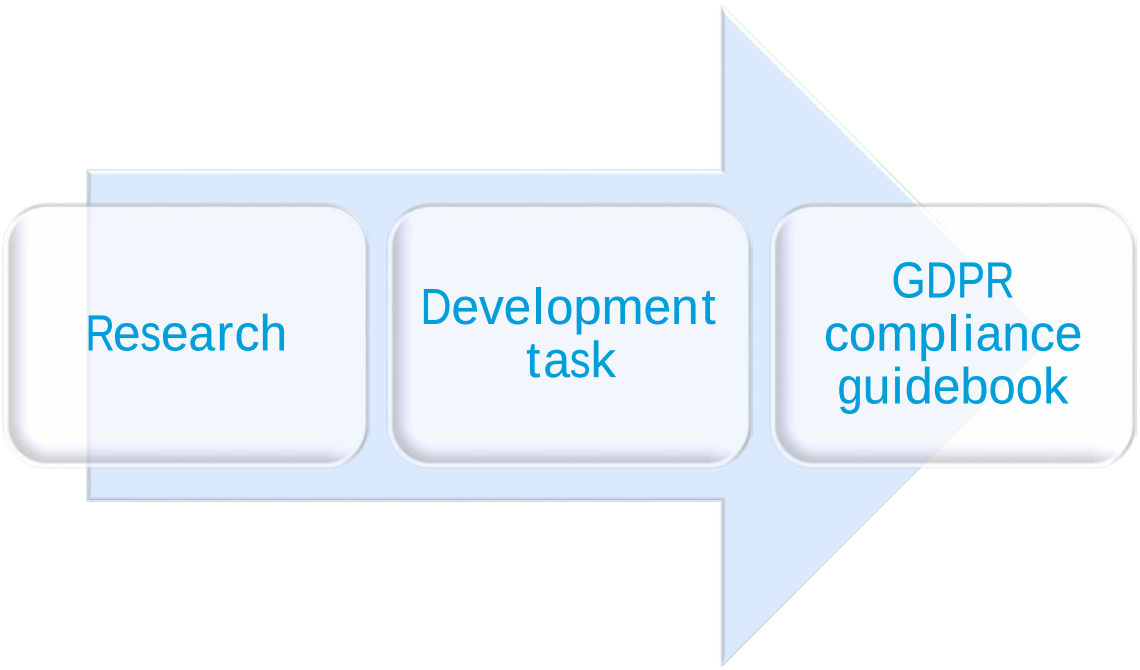

Figure 2: Steps of Thesis Project

3 Earlier research and professional discussion in the field.

The General Data Protection Regulation was enforced on May 25, 2018, thus making this branch of law brand new. In the European Union, GDPR replaces the EU Data Protection Directive 1995. Thus, for the reasons of GDPR being recent enforcement in the European Union, which can transcend to other countries as well because of the concept of territoriality according to Art. 3 of GDPR, Territorial Scope (General Data Protection Regulation (GDPR) 2018), the literature review was conducted to study earlier discussions in the field led by professionals around the European Union, the United States and the United Kingdom. The purpose of this literature review is to study GDPR enforcement in higher education and gather information for the creation of the GDPR compliance guidebook.

The most prominent issue discussed was the lack of experience with GDPR because it was only enforced this year. According to Yeadon (2017), nobody has tested this regulation out yet (Practical applications of GDPR for further education conference 2017). Even though the conference was held in December 2017, there was still not enough time to fully comprehend the regulation.

There were a few cases, where GDPR was violated. One such case happened in Austria, where entrepreneur was fined for how the CCTV cameras were recording the big area of a sidewalk,

which is a violation because the large-scale monitoring of public places violates the GDPR. (Fritz, 2018)

The other case happened in France, where the French Data Protection Authority was investigating the Ad tech area. This company had problems with compliance and French Authority gave them 3 months to bring their processes to compliance before issuing the fines, information provided by Gabriela Zanfir-Fortuna, Data Protection Expert at the GDPR open forum. (Bermann, Grimm, Zanfir-Fortuna, 2018)

These cases give some insight into how GDPR might function in practice, but these cases are not connected to the higher education field and might not be considered directly relevant, however, these cases demonstrate that authorities are ready to enforce the regulation actively and pass the fines for non-compliance.

The maximum fine for GDPR non-compliance is 4% of total revenue, which is why it is important to give this regulation the attention it deserves. (GDPR 2018)

Many professionals in the field of higher education discuss how vague the General Data Protection Regulation is. At the conference on "Practical applications of GDPR for further education", unclear guidance on data retention was mentioned. (Yeadon 2018) As well as at the University of Michigan were questions concerning the fact whether the European Union will provide other countries with GDPR guidance compliance. These discussions demonstrate how important and useful this thesis project could be for other universities and professionals.

Similarly, at the EUNIS workshop for Data Protection and IT Security, (Berlin, 21. April 2017) challenges of new EU-GDPR were mentioned, with the question: "What to do to be legally compliant?" because guidelines are not specific, leaving a room for interpretation. According to this same source (EUNIS workshop), because the aspects remain unclear that leads the application of GDPR difficult and expensive to apply in practice.

Concerning the application of GDPR in the USA, one should take into account the predominantly different approach towards data protection. While in the European Union data protection rights are considered human rights, in the U.S. they are not. At the GDPR Open Forum at the University of Michigan (July 2018), it was suggested looking at the difference between E.U. and U.S. this way (Bermann, Grimm, Zanfir-Fortuna, 2018):

- In the U.S. you can collect data unless the law says that you can't.
- In the E.U. you cannot collect data unless the law says you can.

Might be useful for the bigger picture to know how colleges and universities in the U.S. are looking at GDPR. The approach varied among different universities. At the GDPR Open Forum,

it was mentioned that an unnamed chief information security officer from a (U.S.A. institution) said, "For us, GDPR doesn't matter. We're not paying attention to it; we don't think it truly applies to us. We don't think that anybody will successfully enforce it against us, so literally, we are doing next to nothing." (Bermann, Grimm, Zanfir-Fortuna, 2018)

The GDPR Open Forum mentioned also that other universities jumped immediately to technical implementations. They were trying to figure out how were they able to provide for rights of erasure, rights of data access, consent models. They are spending already probably tens of hundreds of thousands of dollars in things that from a risk-based perspective they don't need to yet, according to Sol Bermann, University Privacy Officer, Interim CISO, U of M (Bermann, 2018). Trying to understand GDPR some are jumping to technical solutions. Some of them may not even really understand what it is that they need to do to comply.

At the same GDPR open Forum Panel, representatives from the University of Michigan were talking about their approach to GDPR. It's one of these situations where it's partly to wait and see. We're doing what we think we need to do from a preliminary perspective. But a lot of this is so brand new, there haven't been any real enforcement actions yet of we know of.

From the ethical perspective, the U.S. universities at least were discussing how concerning it is that E.U. is trying to pass laws that they try to enforce on the rest of the world.

According to the professionals around the world, the GDPR is very unclear and requires time and practice to understand it better. (Bermann, Grimm, Zanfir-Fortuna, 2018) Therefore, the aim of my thesis project should be helpful to clarify some concepts and risks of GDPR non-compliance in practice. As well as to study the regulation further and interpret its concepts.

4 Theoretical framework

During this thesis project in order to create GDPR compliance guidebook for a single University of Applied Sciences in a Southern Finland, the author was working with the legislation such as the GDPR and the officially translated version of Universities of Applied Sciences Act. The General Data Protection Regulation solely is not helpful in the creation of the guidebook for a University based in Finland. To support GDPR legislation, it was decided to use relevant articles from “Universities of Applied Sciences Act”, also known as Ammattikorkeakoululaki 14.11.2014/932 in the Finnish language. The Finnish Data Protection Act or Tietosuojalaki was decided not to use due to the lack of English language translation, however, there is a reference to this act in the guidebook’s text. The following subchapters contain extracts from the law that had been studied and used in the guidebook.

4.1 Universities of Applied Sciences Act 932/2014

In the Universities of Applied Sciences Act, Chapter 6 Section 27 "Access to information relating to admissions", it is stated that regarding the revocation of applicant's right to study, when requested by the University of applied sciences the applicant should provide personal health information necessary for admission. The applicant should provide information concerning the previous decision on revoking the applicant's right to study. (Finlex 2017) According to Chapter 6, Section 27 of the Universities of Applied Sciences Act, the UAS has the right to gather information from other UAS, universities and educational institutions for the purposes of admission.

According to Chapter 6, Section 34, “Access to information relating to revocation of the right to study" of the Universities of Applied Sciences Act, the student must provide information on her or his criminal record entries if the UAS request it for the purposes of assessing the right to study. Additionally, the paragraph states that the student must provide the required by UAS information if the studies or training involve working with minors. According to Chapter 6, Section 34 of the Universities of Applied Sciences Act, the UAS has the right to collect information needed for admission from other UAS or universities, or educational institutions. The information can be regarding a process of revocation of the right to study (mentioned in section 33) when the student applied as a transferred student.

According to Chapter 6, Section 34 of the Universities of Applied Sciences Act, the UAS is bound to inform the National Supervisory Authority for Welfare and Health concerning revocation of the study or other decisions related to that. Additionally, the information regarding the transfer of the student to different studies and reasons why the transfer happened, whenever the information is needed to fulfil the statutory duties of the Authority. According to Chapter 6, Section 36 "Drug testing" of the Universities of Applied Sciences Act, the UAS may require a student to disclose a drug test certificate. In order to make such a request, the UAS must have sufficient grounds or evidence pointing to the fact that student is addicted to drugs while performing practical tasks related to studies or if good judgment and mental acuity are necessary for the student's performance.

According to Chapter 6, Section 40 "Handling of sensitive material of the Universities of Applied Sciences Act, information regarding student's or applicant’s health (a reference to sections 27, 34-36) can only be handled by people who make decisions on admissions, revocation of the right to study, make decisions on disciplinary actions. Additionally, such information can be handled by people who make statements on these matters. According to Chapter 6, Section 40 of the Universities of Applied Sciences Act, the information concerning student's criminal record (as spoken about in section 33(2)) can only be handled by people who deal

with decision making on the revocation of the right to study. According to Chapter 6, Section 40 of the Universities of Applied Sciences Act, the specification of the tasks that include handling of sensitive information is necessary. According to Chapter 6, Section 40 of the Universities of Applied Sciences Act, the university should store sensitive and personal information separately. Any sensitive information should be removed when no longer needed for performing duties or in 4 years.

4.2 The General Data Protection Regulation

Under the General Data Protection Regulation, Art. 5 p. (F) when handling data, the appropriate security of personal data must be ensured. It includes protecting personal and sensitive data from unauthorised processing, unlawful processing, accidental loss, destruction, damage. (GDPR 2018) According to Art. 5. personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. GDPR Art 5, states that personal data must be held for no longer than necessary. Recital 39 "Principles of data processing", quote: "In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review."

In addition, being aware of penalties for careless mistakes can be a good motivator for handling information mindfully. For example, Art. 83 "General Conditions for imposing administrative fines" of GDPR can raise awareness. According to this article, for examples, non-compliance with the provisions will be subjected to administrative fines 10 000 000 EUR or in the case of an undertaking up to 2% of the total annual turnover of the prior fiscal year depending on what is higher.

Additionally, according to the Art. 9 of GDPR, processing of personal data that exposes sensitive details about the data subject is prohibited, however, the GDPR also provides exceptions allowing for such sensitive information to be handled. For example, one such exception applies if processing of sensitive information would be vital in protecting interests of data subject, who cannot give their consent legally or physically. The Member State Law is also mentioned in Art. 9 of GDPR, in which case it will be important to turn to the Finnish National Data Protection Act.

In chapter 4 of GDPR Art., 24-34 are reserved for controller and processor and their obligations. Art. 28 of GDPR specifies as compulsory for binding contracts between controllers and processors. The data controllers are obliged to include a list of compulsory clauses in the contracts with the processors.

All these measures guarantee better protection of data subjects, whose personal data is being outsourced. If there is to be a breach of security due to non-compliance, both the controller and the processor will experience the consequences. When GDPR came into force, the way the contracts were put together between the data controller and data processor had changed. Now, under GDPR, the data controller imposes more obligations on a data processor.

According to Art. 28 GDPR, a processor should provide sufficient guarantees as in "to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject". Other examples that fall under this clause are records of processing activities Art. 30 GDPR, confidentiality, data security (like pseudonymization or data encryption) and the deletion of data.

According to Art. 28 of GDPR, Controller and processor are expected to increase their communication. For example, if the data processor, who is already in contract with data controller wants to work with another processor, who isn't involved with data controller, to begin with, then they (data processors) can't work together without the controller's consent to subcontract. As in Art. 28 GDPR, "the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes".

GDPR has several other matters on which the controller and processor are supposed to cooperate and communicate. For example, instructions are given by the controller regarding the data transfer. The processor is obliged to inform the controller if in their opinion the instructions provided by the controller are about to breach GDPR legislation or a Member state law.

Also, what does the term "the instruction from the controller" mean? The contract between the data controller and the data processor should identify the term precisely. Clear communication between controller and processor should be present on matters such as requests of the data subjects, breach notification and availability of information. According to Art. 28 of GDPR, the allocation of the risk for non-compliance between controller and processor should be present.

According to Art.83, failure to comply will be met with administrative fines, depending on the infringement. If the controller and the processor are both liable for the damage caused by data processing, then both parties will face ramifications. In these cases, the individuals will be in their right to file the compensation claims for both material damage and non-material. Other sanctions can also be involved, according to the General Data Protection Regulation.

According to GDPR Art. 32 Security of processing, it states that controller and processor should be able to create technical and organizational measures to protect the personal information of data subjects. These measures include encryption of personal data and being able to ensure ongoing confidentiality.

Art. 32, GDPR states that controller and a processor should be certain that any person who is working on their behalf and who specifically has the access to personal data, only handles this data according to instructions given to this person by the data controller. The exception, in this case, can be the requirements from the Member State law. According to Art. 32, GDPR, unauthorized disclosure of personal data should be prevented.

5 Methodology

In this chapter of the thesis report, the author will expand on the process of data collection for the GDPR compliance guidebook. In order to create the guidebook, certain methods were used, such as literature review, planning and the implementation of the guidebook, data collection and analysis of the information for the guidebook as well as studying legislation. The chapter will include information on how the GDPR compliance guidebook was structured.

5.1 Literature review

In order to create GDPR compliance guidebook for a University of Applied Sciences, the objective was to research and analyse the GDPR implementation in higher education institutions. The GDPR compliance guidebook is meant to be a helpful guide for the employees of the Universities of Applied Sciences, therefore it's important to investigate the following questions. How do other universities implement the GDPR? How do they work with it? How do they interpret it? In order to find out the answer to this question, a literature review was conducted. The literature review as a research method involved collecting articles and other published or electronic sources, reading these sources and analysing the discovered information, furthermore, synthesising the collected information into the essay. This is a qualitative research method.

For this development project, a literature review was the most valid option of data collection, because it allowed collectively research and analyse many relevant sources in order to get the information, without having to visit a large number of universities or actually contact the data protection professionals for the interview to learn the subject. The following details will demonstrate the system for the literature review.

Searching method

For this thesis project, the electronic sources were used. Through the multiple universities located in the United Kingdom, the United States and other European cities, the search was

conducted to determine if these universities had any information covering GDPR on their websites. Additionally, the search touched any electronic news articles regarding the subject of GDPR in universities. The links found in the websites and articles were also searched for any useful information. Figure 3 (Searching method for a literature review) illustrates the short summary of the searching method in the form of a list.

Figure 3: Searching method for a literature review

Terminology used for the search.

In order to search for relevant information for this thesis project, terms such as "GDPR guidelines", "Universities", "Compliance" were used in different combinations. However, in order to obtain more results during the search for articles and information, the synonyms for each term, "GDPR compliance", "Universities", and "Compliance" were established and utilised, as table 1 (Terminology for a Searching method) below demonstrates. The synonyms then could be used together for a more expanded search. For example, one option for a search would be "GDPR compliance in Universities" and the second option, compiled from the synonyms would be "GDPR recommendations for educational institutions". The first search option yields 514 000 results, while the second one gives 51 600 000 results, thus extending the search.

GDPR Compliance	Universities	Compliance

Data Protection guidelines	College	Obedience to
GDPR instructions	Academy	Accordance with
GDPR recommendations	Educational institutions	Observance of
GDPR advice	Educational establishment	Observation of
GDPR procedure	Institute	Adherence to

Table 1: Terminology for a Searching Method

Inclusion criteria.

During the literature review, not every article found was included in the collective research. Figure 4 (Inclusion criteria for a literature review) below demonstrates how the structured inclusion criteria were used during the work with the sources. In order to be included, the article should be relevant, reliable, informative and the location of the article was important during the selection. The relevance of the article was determined by the content that should have contained information about GDPR compliance in universities. In order to determine if the article is reliable, the names of the authors, the dates and the references, if used should all be listed.

The locations of articles and university websites were considered and selected. According to the advice from the project's client Tiina Ranta, the United Kingdom (UK) universities were the focus of the study due to the high quality of their data protection policies. Additionally, other European countries were also included in the search. The universities of the United States (US) were included because it adds interesting information for the research. It brings in a perspective from a US point of view on how to approach GDPR policies and it can be relevant due to international cooperation between European and American universities, in terms of international research and exchange programs. The articles and university websites should also be informative for the research, and they should contain enough information, a minimum of 2 pages. The exception for this rule would be if a single webpage contains several links with more information on the subject.

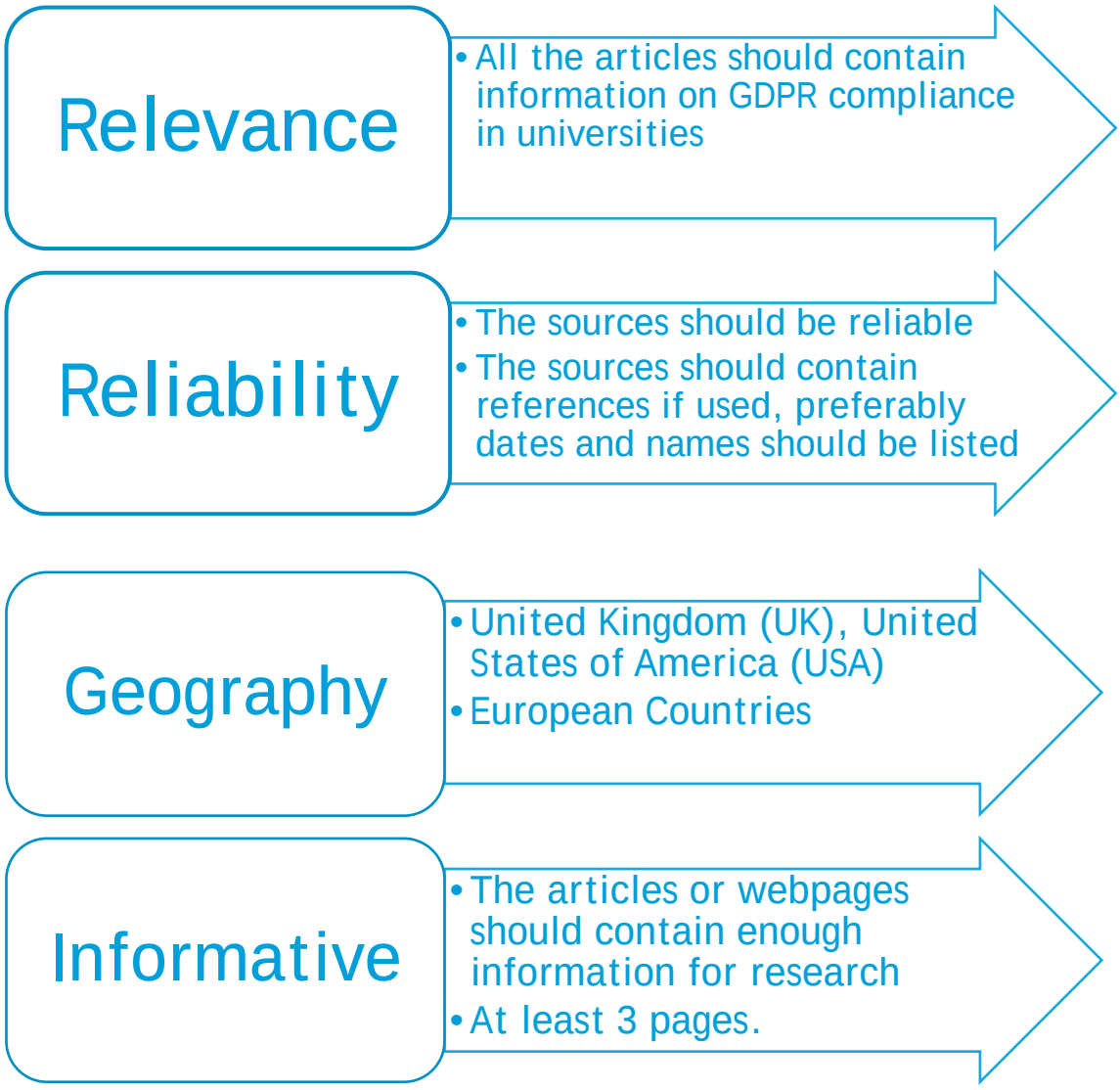

Figure 4: Inclusion criteria for literature review

5.2 Results

The literature review was meant to help in uncovering the information on how GDPR is implemented in Universities. After examining electronic sources and going through the universities' webpages, a comparative analysis was made. Due to comparative analysis between a single university of applied sciences in Southern Finland and Universities in the United Kingdom, a few differences regarding the GDPR implementation were established, or to be more precise, how the GDPR implementation was demonstrated publicly. The primary notable difference was that many Universities in the UK had webpages with information on GDPR, while a single university of applied sciences in Southern Finland didn't have any GDPR webpages on their website.

The webpages contained information regarding GDPR related issues for students and employees. For example, the University of Hull (Data Protection at the University of Hull, 2018) has the entire section on their website, dedicated to Data Protection. In it, they briefly explain how data protection works at the University of Hull, furthermore, they had subsections that concentrate on data subject rights, how we handle personal data of current students, how we handle personal data of current staff, alumni records. In subsections for current students and current staff, they have a "privacy notice" that gives a link to an extensive word document with information on the topic. The website of the University of Portsmouth contains plenty of information on Data Protection. (Data Protection - Corporate Governance: University of Portsmouth. 2018) The University of Portsmouth's presents a comprehensive guide to GDPR, which includes fact sheets and statements with details on subjects such as research and GDPR, legal bases for processing, differences between GDPR and Data Protection Act (DPA) 1998. The website also has a comprehensive guide for anyone who wants to request their data, as well as a guide for students and a guide for staff members. The website organised the guide for staff by giving information for staff as data subjects and staff as data processors.

The University of Stirling in the UK contains a "Data Protection Guidance Handbook" pdf file on their website. (Data Protection Guidance Handbook: University of Stirling. 2018). This PDF file on data protection consists of 39 pages and 17 chapters of information. Below, Table 2 presents the table of contents in order to demonstrate the topics this handbook delves into.

1. Glossary	10. Transfers of Personal Data Outside the EU
2. Personal Data	11. Data Protection Impact Assessments
3. Key considerations	12. Data Protection by Design and Default
4. Data Security	13. Direct Marketing
5. Consent & Privacy Notices	14. Personal Data Breaches
6. Research	15. GDPR Fines
7. Subject Access Requests	16. Personal data processed by students

8. Data Sharing	17 Photographs and recorded images
9. Requests for Personal Information from Third Parties	
Appendix 1 – Template for Privacy Notice	Appendix 4 – Template Consent form for Photography/Filming
Appendix 2 – Data Protection Impact Assessment Form	Appendix 5 – Template notice for Photography/Filming
Appendix 3 – Information required in the event of a Data Protection Breach	Source: (Data Protection Guidance Handbook: University of Stirling. 2018)

Table 2: Table of Contents example for "Data Protection Guidance Handbook"

Additionally, to 17 chapters, the handbook contains 5 Appendices in a form of templates and forms, which should prove helpful and functional to the readers.

Moreover, UK universities let their readers know, who their Data Protection Officer (DPO) is and how to contact them. For example, the previously mentioned University of Stirling, on the last pages of their handbook refers to their DPO, states their name, telephone number and email address. The University of Nottingham, UK shares on their website who was appointed as their DPO. They share that University inaugurated the project that will oversee the GDPR implementation and they introduce the chairperson of the project. (GDPR Overview - The University of Nottingham. 2018) As a result, knowing who works as a Data Protection Officer at the University, will help the reader to navigate faster and contact the right person in case they have a question or any incident to report. The single university of applied sciences in Southern Finland did not contain such information on their website at the time of the research.

6 Developing the guidebook

In this chapter, the development of the GDPR compliance guidebook will be discussed. It was possible to understand the topic of GDPR in higher education facilities better with the help of the research in the form of a literature review, and therefore structure and organise the guidebook. The following subchapters will include the information on the guidebook requirements, how the guidebook was structured and planned. The data collection for the guidebook will be further explored.

6.1 Requirements for GDPR compliance guidebook

The GDPR compliance guidebook was created with the purpose of reducing data protection risks from the general UAS Risk Assessment summary.

The requirements for GDPR compliance guidebook were provided by Tiina Ranta, Director of Safety and Security at Laurea University of Applied Sciences, thesis project's supervisor.

The GDPR compliance guidebook for employees should be written in a clear English language, additionally, the guidebook should be easy to read and understand. The guidebook should be short, around 20 to 40 pages. The supervisor specified that an ideal number of pages would be 20. This requirement demonstrates that the guidebook should be written succinctly and to the point, as well as it shouldn't contain any unnecessary information. The point was made that thick guidebook with too many pages filled with theoretical information and legislation might avert readers from reading it. Therefore, the parts with legislation in the guidebook should contain a minimum of legal language and containing references to the relevant legal sources. Since the guidebook is made for employees it should help them navigate through the legislation instead of teaching it to them.

Additionally, there was a task from a client (T. Ranta) to come up with a few questions for each section. The questions were supposed to promote critical thinking and interest in the topic; however, it was not expected that readers would write answers in response to the questions.

The author was provided with specific structure requirements upon which the layout of the guidebook should be built.

6.2 Structure of the GDPR compliance guidebook

The GDPR compliance guidebook will be based on the highest risks from the summary of UAS risk assessment.

The guidebook contains 4 short sections each related to a certain group of risks. The sections are named according to the risks and the discussion will delve into the topics related to these risks. It will be discussed what is sensitive information and how to handle it, it will contain useful information about data controllers and data processors and more about the security of processing and the importance of data minimisation.

Each section contains legislation. Aside from the general data protection regulation, the Universities of Applied Sciences Act will be used as well. Each section contains real-life case examples as well as recommendations and tips on how to improve the situation or prevent the worst from happening.

The questions at the end of each section are meant to trigger a discussion and critical thinking analysis. The guidebook will not contain answers to these questions because the author doesn't want to restrict anyone's thinking and make it about strictly right and wrong answers.

6.3 Planning the guidebook

The planning stage for the GDPR compliance guidebook happened once the requirements were established during the meeting with the client, Tiina Ranta. The task during this stage was to organise the subjects for data collection, determine the schedule and adjust the structure of the guidebook if necessary. Risk Assessment summary for UAS (2018), provided by Tiina Ranta consisted of 8 risks of high importance. The task was to create 5 sections for the guidebook based on these risks. After inspecting the risks, the author decided to group similar risks or the risks on the same subject together. As a result, Table 3 below (Allocating risks for sections) demonstrates how the risks were grouped and allocated to each section.

Number of the Section	Risks upon which the section would be based
Section 1	• The lack of guidelines for handling sensitive information • The staff does not understand how to deal with sensitive information -

	electronic, verbal, manual data processing • People are sharing sensitive information in public places • Sensitive information is dealt with in systems where it should not be done
Section 2	Outside parties do not adequately protect the information.
Section 3	Sensitive information can be leaked because the legitimacy of the recipient, who requests personal information was not checked.
Section 4	Unnecessary documents will not be destroyed immediately.

Table 3: Allocating risks for sections

The author of the guidebook decided to create four sections instead of five and exclude 1 risk, which was “The backgrounds of staff members are not checked" because the section based on this risk would not be suitable for the GDPR compliance guidebook for employees.

Next step was to structure the sections for the guidebook. The structure should make the sections clear, easy to read and understand, it should be informative and relevant for the employees of Universities of Applied Sciences. Table 4 (Structure of the Section for the GDPR Compliance Guidebook) demonstrates the topics of a section organised and ready for data collection.

Structure of the Section
How is it relevant?
Risks, which define the section

GDPR legislation related to the case
Real-life Examples, looking into the problem more closely
Recommendations
Important points to remember
Questions to discuss

Table 4: Structure of the Section for the GDPR Compliance Guidebook

After the sections were structured and the risks were redistributed among the sections, the titles for each section were created for easier navigation and reference, as Table 5 (Allocating the title for each section) demonstrates.

Number of the Section	Risks	Title of the Section
Section 1	• The lack of guidelines for handling sensitive information • The staff does not understand how to deal with sensitive	Sensitive Information and how to handle it.

	information - electronic, verbal, manual data processing • People are sharing sensitive information in public places • Sensitive information is dealt with in systems where it should not be done	
Section 2	Outside parties do not adequately protect the information.	Data Controller and Data Processor
Section 3	Sensitive information can be leaked because the legitimacy of the recipient, who requests personal information was not checked	Security of Data Processing
Section 4	Unnecessary documents will not be destroyed immediately.	Data minimisation

Table 5: Allocating the title for each section

The schedule for the project work on the guidebook is presented below in table 6.

DATES	PLAN OF ACTION
October - November 2018	Planning and organizing the structure, meetings with Tiina Ranta and Marjo Valjakka
December 2018 - January 2019	Data Collection

February 2019	Writing the text and organizing it
March 2019	Getting the feedback and discussing the results with the client.

Table 6: Schedule for the work on Thesis Project

6.4 Data Collection for a Guidebook

Data Collection for a guidebook consisted of researching and collecting information on real-life cases regarding GDPR violation as well as gathering information for the recommendations. Each section was organized by GDPR subject and supposed to contain real-life case examples and recommendations according to the subject. Table 7 (Sections of the Guidebook by the subject) demonstrates the subjects chosen as the titles of the guidebook.

Sections of the Guidebook by the subject.
Sensitive information and how to handle it
Data Controller and Data Processor
Security of Data Processing
Data Minimisation

Table 7: Sections of the Guidebook by the subject

Initially, according to the plan, real-life cases were supposed to be concerning the GDPR violations, specifically in higher education facilities. However, it proved challenging to find such examples set in universities. There were reasons as to why there were limited numbers of such examples. GDPR was only recently enforced in May 2018, therefore, not many violation incidents happened or were shared with the press. Another fact that would fall under the limitation was that in the news articles these case-studies were reported superficially without going into more details. The lack of certain details made it hard to work with recommendations and overall build the section. Due to the lack of examples from Universities, it was decided to extend the search for GDPR violations to other companies and organizations.

Below, the author will share the searching methods used for data collection, terminology and key phrases, as well as synonyms for terminology. The principles of this research are similar to the ones used in a literature review research.

Searching Method

During the searching process, electronic sources were used. The aim was to find examples among the news articles on GDPR noncompliance.

Terminology and Keywords

These general key phrases, as table 8 (Terminology for data collection for the guidebook) demonstrates, were used during the search for real-life examples for a guidebook. Notably, each key phrase was modified according to the subject for each section, because the task was to find real-life examples for every subject.

GDPR noncompliance examples
GDPR noncompliance among employees
Data breach companies
Common mistakes sensitive data handling

Table 8: Terminology for data collection for the guidebook

Synonyms for the terms and keywords.

The synonyms for the terms, as table 9 (Synonyms for the keywords) below demonstrates, helped to widen the search of real-life case examples in a similar manner as in the literature review search.

Noncompliance	Business	Employees
Breach	Work	Worker
Delinquency	Organisations	Member of staff

Dereliction	Companies	Workforce
Infraction	Line of Work	Personnel
Infringement	Trade	
Neglect	Employment	
Offence		
Violation		

Table 9: Synonyms for the keywords

6.5 Development Project Results

In order to complete the development project, the following goals were accomplished. The structure for a guidebook was created with the help of risk assessment summary for UAS (Ranta, 2018). Each section was logically structured according to the topic. The data was collected for recommendations and real-life examples of GDPR violations at various organizations; these cases were relevant to each section's topic.

Following the project schedule, the text for a guidebook was written and organized in February 2019, thus concluding the development task for this thesis project, which was to create the text for GDPR Compliance guidebook for employees. The requirements provided by Tiina Ranta, as table 10 (Guidebook requirements) below demonstrates, were followed and accomplished successfully.

Requirements for GDPR Compliance Guidebook, provided by Tiina Ranta
Clear and concise English language
Easy to read and understand
Short = 20 to 40 pages
Succinctly written and to the point, no unnecessary information

Minimum legal language
Few questions for each section

Table 10: Guidebook requirements

7 Conclusion

During the work on this thesis project, the author had an opportunity to familiarise herself with the General Data Protection Regulation, how it functions in higher education facilities and what is required in order to comply with it. The research for the thesis project included universities located in the UK, US and those European countries that contained information in the English language, which was a certain limitation. However, due to the novelty of the GDPR, there was a considerable lack of information and research options were limited to what was known about the GDPR at that point in time.

During the research for the project, it was discovered that data breaches happen mostly due to human error, and 84% of data breach incidents were unintentional or accidental. (Sher-Jan, 2018) Therefore, raising awareness among the employees will be an effective measure in reducing the risk of the data breach. GDPR compliance guidebook will serve that purpose of raising awareness while discussing most general data protection risks and how to avoid them. The guidebook does not contain a lot of complex legislation writing because explaining and reiterating legislation will not help the organization to reduce risks, it might lead to the fact that the employees will decide not to read the guidebook. Instead, the GDPR compliance guidebook focuses on real-life cases, which were based on data protection risks, recommendations and tips on how to avoid the data breach. Showing people where mistakes on how to handle sensitive information originate and providing the information on how to deal with it should enforce the GDPR compliance. In general, spreading the information that is easily understood decreases the chances of an accidental data breach.

7.1 Recommendations

These recommendations are based on the results that were uncovered during the research part of the project. After researching how other universities in the United Kingdom (UK) approach GDPR, it has been observed that these universities have a comprehensive GDPR and data protection related webpages with information on their websites. Laurea University of Applied Sciences doesn't have such a webpage on their website; therefore, it is recommended creating GDPR webpage with basic information on data protection for everyone to see and stay in the know about their rights.

Taking into the account another research result, which was that Universities very clearly state who the Data Protection Officer in the university is and how to contact this person if there are concerns, questions or something to report. The author believes that Laurea UAS should adopt a similar approach and identify their DPO on the website as well as the contact details.

One of the limitations of this project was the fact that the General Data Protection Regulation was enforced in May 2018. In this case, it is recommended to improve and upgrade the GDPR compliance guidebook in the future because the implementation is ever-evolving and the real-life cases and recommendations will soon be out of date. With time, more GDPR cases will be available and the implementation of the regulation will be more researched. It would also be beneficial to create an electronic interactive version of the guidebook.

References

Electronic sources

Bermann, S. Grimm, D. Zanfir-Fortuna, G. 2018. University of Michigan - GDPR Open Forum. Accessed 9 Nov. 2018
https://drive.google.com/file/d/18F2tHOVgCu__YVMd4PZANCkvHSFnldDv/view

Data Protection Guidance Handbook: University of Stirling. 2018. Accessed 9 Nov. 2018
https://www.stir.ac.uk/media/stirling/services/policy-and-planning/gdpr/documents/GDPR-Guidance.pdf

Data Protection at the University of Hull. 2018. Accessed 9 Nov. 2018
https://www.hull.ac.uk/choose-hull/university-and-region/key-documents/data-protection.aspx

Data Protection - Corporate Governance: University of Portsmouth. 2018. Accessed 9 Nov. 2018
http://www2.port.ac.uk/departments/services/corporategovernance/dataprotection/

European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, October 1995. Accessed 25 April 2019 https://www.refworld.org/docid/3ddcc1c74.html

Fritz, G. 2018. First GDPR fine issued by Austrian data protection regulator. Accessed 9 Nov. 2018 http://digital.freshfields.com/post/102f39w/first-gdpr-fine-issued-by-austrian-data-protection-regulator?mkt_tok=eyJpIjoiTm1VMFkyUmlOV1V5WkdVMiIsInQiOiJuV25SU25JYlNFT3Q4K244NEQwY01WQ0IwSWhMXC9ZdktDbE9iMXQ1SktXQnBrR0VKMkZMRDBLa1Rka3JPazNLV2syVW5hYkpicW1lODBIan

GDPR Overview - The University of Nottingham. 2018. Accessed 9 Nov. 2018
https://www.nottingham.ac.uk/governance/records-and-information-management/gdpr-overview.aspx

General Data Protection Regulation (GDPR). Accessed 9 Nov. 2018
https://gdpr-info.eu/

Roberts, W. Dolphin, L. FrazziniKendrick, B. 2017. Is Your Institution Ready for GDPR? Posted in Colleges and Universities, Independent Schools, Records (Student Records), Rights of Students. Accessed 9 Nov. 2018
https://www.ctschoollaw.com/2017/12/is-your-institution-ready-for-gdpr/

Sher-Jan, M. 2018. Data indicates human error prevailing cause of breaches, incidents. Accessed 25 April 2019
https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/

Finlex. 2017. Universities of Applied Sciences Act 932/2014. Accessed 25 April 2019
https://www.finlex.fi/en/laki/kaannokset/2014/en20140932

United Nations. 1948. Universal declaration of human rights. Accessed 25 April 2019
https://www.un.org/en/universal-declaration-human-rights/

Yahyapour, R. 2017. New EU-GDPR: Challenges for Universities and Research Organisations. Accessed 9 Nov. 2018
http://www.eunis.org/wp-content/uploads/2017/07/EUNIS-GDPR-YAHYAPOUR.pdf

Yeadon, J. 2017. Practical applications of GDPR for further education, Part of the Jisc GDPR conference. Accessed 9 Nov. 2018
https://www.youtube.com/watch?v=nPXYD7GwaZ0

Unpublished sources

Ranta, T. 2018. Risk Assessment summary for University of Applied Sciences

Appendices

Figures

Tables

Appendix 1: First appendix

THE GENERAL DATA PROTECTION REGULATION COMPLIANCE GUIDEBOOK FOR A SINGLE UNIVERSITY OF APPLIED SCIENCES IN SOUTHERN FINLAND.

Elizabeth Hohtar

2019

Table of contents

Introduction to Guidebook.

Greetings! This guidebook on the European Union's General Data Protection Regulation which came into force in May 2018 in the member states, was created as my bachelor's thesis project. My aim was to research this new regulation, understand it and shed some light on it, therefore helping others to understand it as well. This guidebook is aimed at employees of UAS in Southern Finland.

The guidebook is based on the highest risks for universities and constructed in such a way, so it would be easier to understand what causes these risks and how to improve the situation with personal information protection. The guidebook contains 4 short sections each related to a certain group of risks. The sections are named according to the risks and the discussion will delve into the topics related to these risks. We will discuss what is sensitive information and how to handle it, learn more about data controllers and data processors, as well as talk more about the security of processing and the importance of data minimisation.

Each section contains legislation. Aside from the general data protection regulation, we also touch upon the Universities of Applied Sciences Act. Each section also contains real-life case examples as well as recommendations and tips on how to improve the situation or prevent the worst from happening.

The questions at the end of each section are meant to trigger a discussion and critical thinking analysis. I'm not writing the answers to these questions because I don't want to restrict anyone's thinking and make it about strictly right and wrong answers.

I hope this guidebook will prove its worth and will be informative and helpful.

Section 1 SENSITIVE INFORMATION AND HOW TO HANDLE IT.

How is it relevant?

The University of Applied Sciences is expected to protect the personal and sensitive information of data subjects, i.e. students and employees.

Risks, which define this section.

- The lack of guidelines for handling sensitive information
- The staff does not understand how to deal with sensitive information - electronic, verbal, manual data processing
- People are sharing sensitive information in public places
- Sensitive information is dealt with in systems where it should not be done

GDPR legislation related to the case.

Under the General Data Protection Regulation, Art. 5 p. (F) when handling data, the appropriate security of personal data must be ensured. It includes protecting personal and sensitive data from unauthorised processing, unlawful processing, accidental loss, destruction, damage. Additionally, according to the Art. 9 of GDPR, processing of personal data that exposes sensitive details about the data subject is prohibited, however, the GDPR also provides exceptions allowing for such sensitive information to be handled. For example, one such exception applies if processing of sensitive information would be vital in protecting interests of data subject, who cannot give their consent legally or physically. The Member State Law is also referred to in Art. 9 of GDPR, in which case it will be important to turn to the Finnish National Data Protection Act.

What should not be forgotten are the laws that apply in Universities of Applied Sciences - AMK-laki (932/2014) on the Finnish soil, regarding the handling of sensitive data of the students.

Sections 27, 34, 36 of Chapter 6 of the Universities of Applied Sciences Act, contain some important points regarding sensitive information. Section 40 of Chapter 6 reserved entirely for handling sensitive information.

Looking into the problem more closely. Real-Life Examples

The risks we are looking at in this section are all connected through the same GDPR principle from Article 5. The data should always be retained securely. In these cases, the lack of instructions leads to a number of mistakes in data management.

It is safe to assume that some mistakes or problems prone to occur without guidance on sensitive information and how to handle it carefully. Examples below are provided by Kevin Beaver, an independent information security consultant.

1. Employees tend to keep work-related files on their personal desktops or laptops, so they can continue working on projects outside of the office. The information security consultant was discussing with an HR manager this exact issue. He asked her if she stored any sensitive information on her personal laptop. She wasn't entirely certain but eventually replied negatively. The scan of personally identifiable information (PII) was performed on her laptop to confirm if there was no sensitive information there. However, the scan located over 40,000 records with Social Security numbers, credit card numbers, bank accounts details on her laptop. This is a data breach waiting to happen.
(Example is taken from the article "The Mishandling of Sensitive Data: Do You Really Know What You Don't Know?")

2. Employees are emailing sensitive information to each other.
The attachments of such emails may contain sensitive information in a form of spreadsheets, PDF files, scans or photo images of personal data. The risk that the email can be sent to a wrong recipient or hacked is significant.

3. The most common example, according to security consultant, is to store database files with sensitive information on an unsecured system like the open network share.
According to the developer from this example, the sensitive information there was outdated, which conveyed the message that because it was old, the sensitive data on these files stopped being sensitive. However, sensitive data can't be outdated and become less sensitive or unimportant.
Also, notice, that according to GDPR the old unnecessary documents should not be retained for longer than necessary, they should be destroyed. This example is relevant to Section 4.

Recommendations.

Perhaps, the good place to start will be defining the term "sensitive information". What makes certain information sensitive? And is there a difference between personal and sensitive information? The answers to these questions are important to be aware of. Once the definitions are clear, it becomes easier to manage data in a secure manner. Quoting the GDPR, Art.4 "Definitions" on 'personal data', it "means any information relating to an identified or identifiable natural person", or in other words, information that can help you to identify the person.

For example, the email address "name.surname@universityABC.fi" is a piece of personal information because it contains a name and a surname of the individual that works for this university. This piece of personal data helps to identify or find a particular person.
Therefore, full names, ID numbers, e-mail addresses and home addresses, bank account details, birthdays, cell phone numbers, physical descriptions, anything that helps to identify an individual is considered personal information.

What about sensitive information? According to IT governance Blog and the author Luke Irwin, if a sensitive data is exposed it will not only identify an individual, it will endanger that individual's wellbeing by leaving an open door to harassment, prejudice, bullying and discrimination. Which is why it is important to pay extra attention to the safety of sensitive information.
Such information includes, but not limited to race, religion, political opinions, criminal record, sexual orientation, ethnicity, genetic data, biometrics and any medical record.

Once one is aware of the impact the revealed sensitive information can have on an individual's wellbeing and life, employees will be able to control how they handle it. Below are some tips and advice.

Looking back to the list of risks, we can assume there's a problem with understanding how to handle sensitive data and how to transmit this data securely. One of the mistakes is to be careless of when and with whom you choose to talk about sensitive information. As a result, people tend to share sensitive pieces of information in public places. An employee should always be careful that the sensitive information they possess is not passed on to third parties in any way, which includes oral communication, electronic or in writing.
So, what you don't want to happen, is for unauthorized parties to overhear or access personal data.

Some important points to remember:

- *When it comes to discussing sensitive information with someone, it's best to find a private place for this purpose, where nobody can overhear your conversation by accident or on purpose.
- *If any notes are made during this private conversation, they should be handled with care and proper security.

- *Don't leave any notes or paperwork with sensitive information unattended, or behind, or where anyone else can read it.
- *If you don't need this information or paperwork, then make sure it's destroyed.
- Remember, that according to the General Data Protection Regulation, Article 5, personal data must not be held for longer than necessary. But also, if you are destroying paperwork you don't need anymore, you must make it in a legal way with an appropriate level of security, depending on the information that you destroy
- *Ensure that you keep personal and sensitive information secure on electronic devices. If it's on the computer or laptop remember to lock the devices when you are leaving, and if you have someone in the office who shouldn't see the information, lock the computer you're working on.

- *Working with personal data on electronic devices and emails, remember to change passwords frequently.

If you are transmitting personal data via the email address or physical envelope, make sure you are careful. For example, depending on the policies you have at your workplace concerning data management, be sure to follow it when handling the sensitive information. If you don't know the policies, it's best to find out how exactly your employer prefers to handle such cases. For example, in general, some workplaces might require approval for the transmission from the employer. If the data is being sent through the email, then it should be marked as confidential as well as encrypted. It's possible that a password to access the data should be sent separately.
Another example, if data sent by a physical envelope, then the recipient should be notified that the envelope with a certain sensitive data is on its way, and the envelope should be properly sealed.
These examples and general tips are provided by "Procedures for handling personal information under the data protection act 1998".

To discuss:

1. Can you find similarities regarding sensitive information between the General Data Protection Regulation and Universities of Applied Sciences Act?
2. In example number 1, security consultant asked the HR manager if she was keeping any work-related sensitive information on her personal laptop. She replied negatively but the consultant found a lot of sensitive information there. How do you think it happened? Why didn't she realise that her laptop contained this information?
3. Think about the significance of sensitive information. Consider how it differs from personal information. Can you predict the consequences of disclosing student's sensitive information to a third party? How will such a leak endanger a student?

Section 2 DATA CONTROLLER AND DATA PROCESSOR

How is it relevant?

The University of Applied Sciences is a data controller. Employees of UAS are working for Data controller. The university hires data processors to work with the data, all the while protecting their students' rights, also known as data subjects.

Risks, which define this section

Outside parties do not adequately protect the information.

GDPR legislation related to the case.

Art. 5. personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
GDPR, Art. 32 regarding the security of processing, is relevant to this topic.
Chapter 4 of GDPR Art. 24-34, reserved for controller and processor and their obligations.
Knowing the differences between the controller and processor and being aware of responsibilities can help to reduce the risk of the sensitive information breach.
In addition, being aware of penalties for careless mistakes can be a good motivator for handling information mindfully. For example, Art. 83 "General Conditions for imposing administrative fines" of GDPR can raise awareness.

Legal requirements.

The example of Contract template can be found at GDPR website. Here is the direct address to the template for your kind perusal.

https://gdpr.eu/wp-content/uploads/2019/01/Data-Processing-Agreement-Template.pdf

Here is what Art. 28 of GDPR specifies as compulsory for binding contracts between controllers and processors. The data controllers are obliged to include a list of compulsory clauses in the contracts with the processors.

All these measures guarantee better protection of data subjects, whose personal data is being outsourced. If there is to be a breach of security due to non-compliance, both the controller and the processor will experience the consequences.

When GDPR came into force, the way the contracts were put together between the data controller and data processor had changed. Now, under GDPR, the data controller imposes more obligations on a data processor. The clauses now included in the contract are, as listed below:

1. Technical and organizational measures imposed on the data processor.

According to Art. 28 GDPR, a processor should provide sufficient guarantees as in "to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject". This is where it is important to carefully consider a data processor before going into business with them.

Other examples that fall under this clause are records of processing activities Art. 30 GDPR, confidentiality, data security (like pseudonymization or data encryption) and the deletion of data.

2. Controller and processor are expected to increase their communication.

For example, if the data processor, who is already in contract with data controller wants to work with another processor, who isn't involved with data controller, to begin with, then they (data processors) can't work together without the controller's consent to subcontract. As in Art. 28 GDPR, "the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes".

GDPR has several other matters on which the controller and processor are supposed to cooperate and communicate. For example, instructions are given by the controller regarding the data transfer. The processor is obliged to inform the controller if in their opinion the instructions provided by the controller are about to breach GDPR legislation or a Member state law.

Also, what does the term "the instruction from the controller" mean? The contract between the data controller and the data processor should identify the term precisely.
Clear communication between controller and processor should be present on matters such as requests of the data subjects, breach notification and availability of information.

3. The allocation of the risk for non-compliance between controller and processor.

Which party is responsible for the risk in case of a data breach or other GDPR violation? What is the risk for non-compliance for controllers and processors?
According to Art.83, failure to comply will be met with administrative fines, depending on the infringement.
If the controller and the processor are both liable for the damage caused by data processing, then both parties will face ramifications. In these cases, the individuals will be in their right to file the compensation claims for both material damage and non-material.
Other sanctions can also be involved, according to the General Data Protection Regulation.

Looking into the problem more closely. Real-Life Examples

A good example of a data breach with such a risk involved could be when the data controller (university) outsources some work to third-party data processors. Such service providers could include but not be limited to law firms, accountants, IT related firms. Some of these service providers have access to highly sensitive information, for example, accountants have the right to access certain sensitive financial data. According to P. Baker and R. Allen, many businesses outsource their key elements to third parties, relying on them increasingly every year. For example, many rely upon cloud data providers with their data retention.
Here is one of the case-examples with a cloud security breach. The cloud-based company Dropbox was involved in a severe data breach in 2012. More than 68 million user accounts with email addresses and passwords were hacked into. That would be almost 5 gigabytes of data. The stolen data were sold at a dark web marketplace for bitcoins. Back then, the price in dollars equalled to about $1141. The company's response to it was site-wide password reset.
If the legitimacy of these firms is not checked or the legal contracts don't include all the necessary obligations set by General Data Protection Regulation, then the data controller can endanger the safety of personal or sensitive information of their data subject.

Recommendations

In this section, the prime focus is on data controllers and data processors. So, what do these terms mean? In the case of the University of Applied Sciences, the data controller would be the university. The university will determine why and how personal data should be processed. The data processor will be any person or company who processes personal data on the data controller's behalf. This will not include the employees of the Data Controller.
Data processor can be, as mentioned earlier in this section, any third-party business or a freelancer. These could be data analysts, accountants, lawyers, data storage on third-party servers and more.
The data controller is obliged to use only data processors, who will be complying with GDPR Art 28, paragraph 1 and will ensure compliance through a binding contract. In this contract, both parties i.e. data processor and data controller will be making sure that appropriate measures are set in place.

To minimise the threat, P. Baker and R. Allen (Disputes 2018: Cybersecurity - risks when outsourcing, partnering and using professional advisors) recommend the following steps for data controllers.

1. Risk assessment and data access review, making sure that only the right party has access to certain sensitive information.
2. Security assessment of a data processor to make sure they are complying with GDPR Art. 28 and have all technical and administrative measures in place.
3. The binding contracts should contain all the relevant standards. Reviewing these standards is highly recommended.
4. It's useful to have a monitoring system. This should help to oversee the incident reports from data processors, make sure the appropriate responses take place, and all procedures are followed.

To discuss:

- The clauses included in a contract according to GDPR are - technical and organizational measures imposed on data processors, increased communication between controller and processor, and allocation of the risks between controller and processor. How, do you think, each of these clauses will help to improve data protection?
- In this section's example, the company's response to the data breach was site-wide password reset. Do you think it was enough? As a potential customer, what kind of response in terms of security and customer services would you expect to see in a similar situation?

- As you have noticed, the recommended steps from Baker and Allen are for data controllers only. What steps do you think data processors should take on their side to minimise the threat?

Section 3 SECURITY OF DATA PROCESSING

How is it relevant?

The University of Applied Sciences as a data controller is expected to ensure secure data processing of their data subjects.

Risks, which define this section.

Sensitive information can be leaked because the legitimacy of the recipient, who requests personal information was not checked.

GDPR legislation related to the case

In this section, we will need to investigate the Universities of Applied Sciences Act as well as into the General Data Protection Regulation. In Universities of Applied Sciences Act, Chapter 6, §40 on Handling sensitive information, it is stated that certain sensitive information, like student health information or police registers, can be only accessed by people who handle student admittance, the right to study or disciplinary issues. This shows that not every single employee has the right to access and handle sensitive information.

If we inspect GDPR Art. 32 Security of processing, it states that controller and processor should be able to create technical and organizational measures to protect the personal information of data subjects. These measures include encryption of personal data and being able to ensure ongoing confidentiality. The university as a controller must take organisational steps to make it clear who has the right to access and handle sensitive information.

Art. 32, GDPR states that controller and a processor should be certain that any person who is working on their behalf and who specifically has the access to personal data, only handles this data according to instructions given to this person by the data controller. The exception, in this case, can be the requirements from the Member State law.

According to Art. 32, GDPR, unauthorized disclosure of personal data should be prevented.

Looking into the problem more closely. Real-Life Examples

The breach of sensitive information can have both direct and indirect consequences to the business. Such incidents can hurt the reputation of the organization in the field, which can be bad for business, and of course, GDPR penalties and sanctions can have this direct blow to financial side and business operations.

So, what can be the cause of sensitive information leakage? Here are some of them, according to Tony Abou-Assaleh (Confidential Information Leaks and Your Employees from Titan File):

1. Employees tend to share sensitive information by accident
2. It could be a malicious insider threat, where employees steal the information.
3. Information can be shared and transmitted via different devices and tools. The low level of security on these devices can result in an information security breach.
4. Careless handling of personal information when the data is sent by mistake to people who shouldn't have access to it.

According to Long Cheng, Fang Liu, and Danfeng (Daphne) Yao (Enterprise data breach: causes, challenges, prevention, and future directions), the accidental leaks of information had increased. Australian Red Cross Blood Service employee accidentally exposed the sensitive documents of more than 550 000 blood donors. Documents were put on their website, which was not only unsecured but also open to the public. These documents contained sensitive information of donors from 2010 - 2016, exposing names and addresses, dates of birth as well as information on drug use and sexual activities, not excluding medical records.
A similar mistake was made in 2011 by a Texas State, which made sensitive information of 3.5 million citizens accessible online.
These are the examples of mistakes made by employees in the organizations. Unfortunately, the examples don't report any details, such as, if these employees had the right to access the data or not. However, if access to sensitive information is not limited, the risk of repeating these mistakes increases.

Recommendations

To avoid the risk presented in this section, the access to sensitive information should be limited to employees who can't perform their duty without this information, i.e. they have a "need-to-know" basis to access the data. Here is some basic security advice to ensure the safety of sensitive information. We are discussing two types of storing information, electronic and physical. In the case of physical documents - they should be locked away from general access, where they can be accessed only by employees on a need-to-know basis. The electronic documents should be password protected.

Here are some tips on how to prevent security breach regarding personal information.

1. The information security specialist (Tony Abou-Assaleh) recommends conducting security checks of employees not only before they are hired but also after they left the employment to prevent threats and ensure the employment is terminated on good terms. The satisfied

employees leaving the place of employment behind are less likely to cause any problems, according to the expert opinion.
2. If the ex-employees have had the right to access sensitive information, then it is highly recommended to change all the passwords.
3. If sensitive information leaves the organization, then this information should be monitored regularly.
4. HR and IT should have good communication and cooperation, working together so sensitive information is even better protected.

Another important advice is not to cut off the flow of information to employees entirely. This tactic will not prevent future data leaks, rather create bottlenecks in day-to-day operations. If certain employees need access to personal information for work purposes, then they should have access to it. The best strategy for preventing sensitive information leaks, which happens quite often by accident, is to raise awareness among inside the organization. Training the staff and providing appropriate skills will also lower the risks of security-related mistakes. Here are essential attributes regarding security controls as per Laura Vegh, Chief Security Officer and the author of the article "How will GDPR change the approach to security?"
1. Confidentiality - "need-to-know" basis access rights
2. Integrity - The data is accurate and complete
3. Availability - the data is available for processing if the business requires it
4. Resilience - The data must be able to recover shall the threat or any mistake occurs
All these attributes should work together to ensure a smooth security process of an information system.

A few Questions

- The examples and the expert opinion in this section demonstrate that the sensitive information breach happens often by accident, i.e. when employees would share some piece of sensitive information when they shouldn't. These accidents and general mistakes are the far more common cause than a malicious threat. Can you name a few reasons why employees would make such mistakes? What is a common thread in your opinion?
- If it was up to you, what do you think is the best tactic to combat an accidental sensitive data breach among the employees and why? Consider other mistakes made by the staff that can lead to a data breach as well.

Section 4 DATA MINIMISATION

How is it relevant?

To comply with the General Data Protection Regulation, the University of Applied Sciences must take measures, which will help to regulate data storage. If personal information is not needed, then it should be disposed of securely.

Risks, which define this section

Unnecessary documents will not be destroyed immediately.

GDPR legislation related to the case

GDPR Art 5, states that personal data must be held for no longer than necessary.
Recital 39 "Principles of data processing", quote:
"In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review."

Looking into the problem more closely. Real-Life Examples.

According to the report from Zack Whittaker from TechCrunch, the 10 years of mortgage documents were exposed online after a security breach on a server. The mortgage documents contained sensitive information and were left on the unprotected server for approximately two weeks. How many people this leak affected is not reported. The source shared that more than 24 million mortgage and banking documents were exposed online.
The TechCrunch's report shared; the unprotected server exposed more than 10 years amount of data. The documents contained sensitive information such as loan agreements, payment schedules, financial and tax reports. The report also states that financial documents were dated back to 2008. As any mortgage documents, these files contained high-level sensitive information, including Social Security numbers and the likes of the information usually found on such documents.
This case can be found in detail on the Techcrunch website, under the article "Millions of bank loan and mortgage documents have leaked online." The example demonstrates not only the dangers of exposing old sensitive information, which now, according to GDPR should be destroyed but also other risks discussed in this guidebook. For example, the lack of protection from the outside party from section 2.

Recommendations

The General Data Protection Regulation now requires adhering to data minimisation principles. According to the legislation, personal data should be deleted when no longer needed. The requirements are strict. Not only it concerns the time of keeping the data, but also its volume. This should help with more efficient data management and cleaner data storage. The older records might become irrelevant and inaccurate and that can lead to certain problems and misunderstandings in business. Noteworthy the fact, that it is much more difficult to protect heaps of personal information when outdated documents are included. Minimizing the data allows maintaining the focus on important up to date documents.
The sensitive information should be disposed of in a secure and proper manner. If the paper documents contain sensitive information, it would be risky to just throw it into a garbage bin. Alternatively, electronic data can be recovered if not destroyed specifically in a secure manner. Identity Theft Resource Center reports that it's common among employees not to dispose of sensitive information securely.
Proper physical destruction requires partnering up with document destruction companies, which should provide services for paper shredding as well as disposing of electronic documents and hard drives.

What kind of information should be destroyed? Here is the list.
Documents regarding employees or customers that contain such information as

- Names
- Mailing address as well as e-mail address
- Important numbers like social security, credit card, driver's license.
- Telephone and cell phone numbers
- Hiring documents
- Photos or physical descriptions
- Personal property information

The second list concerns sensitive information related to University matters. Any information collected from the students. For example, here is what University of Portsmouth collects from their students. Any information like this, shouldn’t be held for longer than necessary.

- Student's name
- Contact details (address, e-mail, telephone numbers)
- Emergency contact details

- Date of birth
- Nationality and country where the student was born
- Academic qualifications if any
- Details of any disability
- Details of any criminal convictions
- Fee information and sponsorship details

Advice on managing paper documents more efficiently, according to L. Hilinski (Breaches from paper files). Below are tips on how to improve the safety of physical documents. Nowadays, digital files reign supreme over physical hard copies, but one shouldn't forget to extend the security measures to physical paper documents.

Document Retention Schedule.

Any organization has a different amount of records, where each document usually has its own expiration date. The retention schedule could help employees with keeping track of these files, knowing when the documents are not needed anymore and when exactly they should be disposed of securely. Having a plan and a catalogue will reduce data breach risks. Such risks can occur if outdated documents are simply forgotten and not destroyed. Where will they eventually end up?

Shredding the documents.

The next step once the schedule was established and employees are aware of the documents' date expiration, then these documents should be consistently destroyed, for example, shredded by a professional company that deals with secure document disposal. The services of such a company should be recurring, following the regular schedule.

Regular Security training.

Regularly educating and training the employees regarding document security should raise awareness and reduce possible mistakes in handling the disposal of sensitive information.

Audit Security systems.

Check in on how the established system works. Are the rules followed? Make sure every system that has something to do with the paper document management is audited. That can include the storage system, mailing system, destruction system. Auditing will help to improve the system once the weak points in certain processes are identified.

To discuss:

- Consider all the examples in 4 sections. Can you find similarities among these cases? Can you find additional GDPR violations in these examples?
- Do you think regular security training for the employees is an effective preventive measure? Can you think of any pros and cons of such measure?

Summary, some important points and tips.

- Data should only be collected for specified purposes and limited to what is necessary for these purposes.
- Data controller and data processor should provide necessary measures for secure data retention.
- Data audit will help to oversee privacy policies, security systems and data minimization, making sure everything is up to date and systems run smoothly.
- Taking the risk-based approach, use data audit to identify where is the biggest risk present, then focus on mitigating it.

- Data protection clauses used in supplier agreements, both in templates and live negotiations, must be reviewed and mandatory GDPR clauses should be included.
- As per contractual terms and conditions make sure to assign legal responsibilities among partners.
- Here are some examples of potential interactions that may involve the collection and use of personal data of EU data subjects: student recruitment, admissions activities, study-abroad programs, faculty and staff recruitment, international research activities.
- Disclosing sensitive information could leave data subject vulnerable to harassment, discrimination and abuse.
- Personal data should not be kept for longer than your organization needs it.
- Consider and justify the length of time for keeping personal information.
- Set a standard retention period whenever you can.
- Review the data often. It might require erasure or anonymisation.
- Remember that according to GDPR, individuals have a right to erasure, if the data is redundant.
- As for the right to erasure, there is an exception, however. The personal data can be kept for longer if kept for public interest archiving, scientific and/or historical research, statistical purposes. - GDPR art 5 (e)

References

1. Guide to Data Protection / For organisations: Principle (e): Storage limitation. Accessed Jan. 2019
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

2. General Data Protection Regulation (GDPR). Accessed 9 Nov. 2018
https://gdpr-info.eu/

3. Whittaker, Z. 2019. Millions of bank loan and mortgage documents have leaked online. Accessed 20 Feb. 2019
https://techcrunch.com/2019/01/23/financial-files/?guccounter=1

4. Data Breaches | University of Limerick. Accessed Feb. 2019
https://ulsites.ul.ie/corporatesecretary/data-breaches

5. Hilinski, L. 2018. Are There Holes in Your Security Strategy? (Breaches from Paper Files). Accessed Feb. 2019
https://www.shrednations.com/2018/01/holes-information-protection-breaches-paper-documents/

6. Valdetero, J. 2017. How Employers Can Become Experts at Data Breaches: Tossed Files. Accessed Jan. 2019
https://www.bclplaw.com/en-GB/thought-leadership/how-employers-can-become-experts-at-data-breaches-tossed-files.html

7. Tips for containing and reducing the risks of a privacy breach - Office of the Privacy Commissioner of Canada. 2018. Accessed Jan. 2019
https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/c-t_201809_pb/

8. McElhill, D. GDPR Data Retention Quick Guide - Data Protection Network. Accessed Jan. 2019
https://www.dpnetwork.org.uk/gdpr-data-retention-guide/

9. d'Angelo, M. Reisch, O. 2016. Outsourcing contracts under the General Data Protection Regulation: more revolution than evolution. Accessed Jan. 2019
https://www.lexgo.lu/en/papers/ip-it-telecom/it-law/outsourcing-contracts-under-the-general-data-protection-regulation-more-revolution-than-evolution,108155.html

10. Cheng, L. Liu, F. Yao, D. 2019. Enterprise data breach: causes, challenges, prevention, and future directions. Accessed 20 Feb. 2019
https://onlinelibrary.wiley.com/doi/full/10.1002/widm.1211

11. Don't let your data fall into the wrong hands. 2014. Accessed 20 Feb. 2019
https://www.guardiandatadestruction.com/dont-let-your-data-fall-into-the-wrong-hands/

12. Procedures for handling personal information under the data protection act 1998. 2008. Accessed Jan. 2019
https://nationalarchives.gov.uk/documents/procedures-feb08.pdf

13. Harel, S. 2018. Enterprise Security: Cloud-y With a Chance of Data Breaches. Accessed Feb. 2019
https://securityintelligence.com/cloud-security-with-a-chance-of-data-breaches/

14. Barhamgi, M. Bandara, K. Yu, Y. Belhajjame, K. Nuseibeh, B. 2016. Protecting Privacy in the Cloud: Current Practices, Future Directions. Computer, 49(2) pp. 68–72. Accessed Dec. 2018
https://oro.open.ac.uk/44987/1/On%20Protecting%20Privacy%20in%20the%20Cloud.pdf

15. Brandel, M. 2010. Cloud security in the real world: 4 examples. Accessed Dec. 2018
https://www.cio.com.au/article/350063/cloud_security_real_world_4_examples/

16. Armerding, T. 2018. The 18 biggest data breaches of the 21st century: Security practitioners weigh in on the 18 worst data breaches in recent memory. Accessed Dec. 2018.
https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

17. Elshof, M. Breedijk, B. Van Es Dentons, C. 2017. GDPR Update: Transfer of Personal Data (outside the EEA). Accessed Dec. 2018
https://dentons.boekel.com/en/insights/alerts/2017/november/22/gdpr-update-transfer-of-personal-data-outside-the-eea?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

18. How to deal with employees who leak confidential information and or company data / Peninsula UK. 2011. Accessed Dec. 2018
https://www.peninsulagrouplimited.com/blog/how-to-deal-with-employees-who-leak-confidential-information-and-or-company-data/

19. The most infamous data breaches. 2019. Accessed Feb. 2019
https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

20. Security Breach Examples and Practices to Avoid Them. 2015. Accessed Feb 2019
https://its.ucsc.edu/security/breaches.html

21. Rothke, B. 2009. Why Information Must Be Destroyed. Accessed Feb 2019
https://www.csoonline.com/article/2123705/privacy/why-information-must-be-destroyed.html?page=2

22. Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). 2018. Accessed Dec 2018
https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

23. Kroman, R. Updated 2017. Ten ways to protect your confidential information. Accessed Jan 2019
https://www.theglobeandmail.com/report-on-business/small-business/sb-managing/how-to-protect-your-confidential-information/article16072896/

24. Why is Confidentiality Important? 2010. Accessed Feb 2019
https://www.halpernadvisors.com/why-is-confidentiality-important/

25. 5 ways to manage confidential and sensitive information. 2017. Accessed Jan 2019
https://blog.v-comply.com/5-ways-manage-confidential-sensitive-information/

26. Employers' access to emails and private files. 2017. Accessed Jan 2019
https://www.datatilsynet.no/en/privacy-and-society/personvern-pa-arbeidsplassen/employers-access-to-e-mails-and-private-files/

27. Vegh, L. 2017. How will the GDPR change the approach to security? Accessed Jan 2019
https://eugdprcompliant.com/will-gdpr-change-approach-security/

28. Abou-Assaleh, T. 2018. Confidential Information Leaks and Your Employees. Accessed Jan 2019
https://www.titanfile.com/blog/case-of-confidential-information-leak/

29. Does your company know which documents to shred? Accessed Jan 2019
https://www.intellishred.com/documents-to-shred/

30. Beaver, K. 2015. The Mishandling of Sensitive Data: Do You Really Know What You Don't Know? Accessed Jan 2019
https://securityintelligence.com/the-mishandling-of-sensitive-data-do-you-really-know-what-you-dont-know/

31. Irwin, L. 2018. The GDPR: Do you know the difference between personal data and sensitive data? Accessed Jan 2019
https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data

32. Mackie, J. 2018. Personal vs. Sensitive Information. Accessed Jan 2019
https://termsfeed.com/blog/personal-vs-sensitive-information/

33. Lichtenberg, C. 2017. What's the Difference Between Personal and Sensitive Information? Accessed Dec 2018
https://legalvision.com.au/difference-between-personal-and-sensitive-information/

34. What is the difference between personal data and privacy-sensitive information? Accessed Dec 2018
https://www.zivver.eu/en/blog/difference-between-personal-data-and-privacy-sensitive-information