LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

GDPR compliance check for Ecommerce platforms

Ville Suokannas

Laurea University of Applied Sciences

GDPR compliance check for e-commerce platforms

Ville Suokannas
Business Information Technology
Bachelor's Thesis
May, 2019

Laurea University of Applied Sciences **Abstract**
Business Information Technology
BBA

Ville Suokannas

GDPR compliance check for e-commerce platforms

Year 2019 Pages 46

The purpose of this thesis project was to identify missing points from the company X's electronic commerce platforms with regard to the new General Data Protection Regulation (GDPR). This was done by summarizing the main points of the GDPR, comparing the new regulation to the old one and auditing 2 platforms that the organization owns.

The knowledge base of this thesis report is based on interviews, case study research, the VAHTI auditing tool and best practices to adhere to the law.

The tests consisted of checking the compliance status of the 2 e-commerce platforms of the organization to uncover missing parts that are mandatory for the GDPR compliance. The first test found that the GDPR statement of the company was missing. As the aim is to be 100% compliant, the first test can be considered a failure.

As the research progressed, the compliance test uncovered areas that are missing from the platforms by comparing the platforms to the compliance list of the auditing tool that was used. These were noted and informed to the owners of the platform so that they could be implemented in compliance with the new regulation. In the second test the problems noticed in the first test were corrected, making these platforms compliant with the new regulation. The success ratio was 50%.

The communication between the platform owners and the researcher was good. Details provided by the interview gave clear picture on the working of the platform and the VAHTI tool assisted in making the test successful.

Key words: GDPR, VAHTI, E-com.

Table of Contents

1 Introduction 6
2 The General Data Protection Regulation 7
2.1 Data subject, Data controller and Data processor 9
2.2 Personal data and the definition of processing 10
2.3 Personal Data Lifecycle 11
2.4 The difference compared to the previous regulation 12
2.5 The rights of the data subject 13
2.6 The duties of the data controller. 15
2.6.1 Basis of Law 15
2.6.2 Privacy by default 16
2.6.3 Data Security Management 17
2.6.4 Notification and collaboration 18
2.6.5 Data transfer outside off Europe 19
2.7 Data processor responsibilities 20
2.8 Agreements and the dividing of duties 21
2.9 Comparison between the previous directive and GDPR summary 22
3 Audit Process 24
3.1 Audit 24
3.2 Vahti-tool 26
3.3 Information classification and the team. 27
3.4 Testing of creating an account 28
3.4.1 Test 31
4 Results 38
5 Conclusions 40

Terminology

GDPR	General Data Protection Regulation
Ecom/Ecommerce	Electronic Commerce Platform
IOT	Internet of Things
PHP	Scripting language for web developing
MySQL	Database management system
XML	Markup Language
XLS	Excel Format
JSON	JavaScript Object Notation, a lightweight data-interchange format.
PDF	Portable Document Format
B2C	Business 2 Customer

1 Introduction

On the 27th of April 2016, the European Union accepted the unification of international Data Protection regulations inside of the EU. This regulation will set forth a broader set of responsibilities and duties for the processors and handlers of the person registries and rights for the people within these registries. As of now this regulation is in effect, but it has been given a transition period until the 25th of May 2018 before it needs to be complied. Organizations and companies that have not even started the change process, as it is required by the GDPR, they will then face a noticeable notch in the competitiveness and in their own operations when their customers start to demand compliance to the law.

The company that this thesis work is for is a Sporting Brand Organization. Their main business is selling sporting goods with cloud connectivity components that the customer can use to track their sporting activities and sport enhancing clothing and equipment. For the company's continuation of their business activity, it is highly critical to prove that their data protection levels in their business activity, as well as in technical environment, is compliant with the GDPR. This is to make sure that customers trust the company and for legal liabilities within the regulation.

The main research questions in this thesis is to map out the situation of the company's data protection, audit their e-com system and, if necessary, create a plan revolving around the EU GDPR requirements that are still missing from the core systems of the organisation and fix them.

The thesis is structured in the following way: in chapter 2 the thesis will cover the technical part of the regulation and make it more feasible for the reader to understand. In chapter 3 the thesis will cover the audit process in a couple of sections, such as the information systems that the company uses to protect their databases and customers data, creation of an account within the e-com

portal to map out the process behind the data needed for an account, questions regarding data changes to the team responsible of handling the database, data portability and deletion.

2 The General Data Protection Regulation

The European Parliament and council decided on the 27th of April 2016 to introduce a new regulation that will protect peoples' private data around the European Union. The regulation is called General Data Protection Regulation (GDPR) The regulation was implemented in May 2016 and it was applied after the 25th of May 2018.

The idea behind GDPR is to unify and synergize the EU countries data regulation laws. Especially it will strengthen the private person's status in data processing and specifies the tasks and responsibilities of personal data processing organisations. The VAHTI-report published by the Ministry of Finance (1/2016) has emphasized the increase in digitalization, new technologies and services and their growths requirements for the utilization of the private data and the need to conduct data privacy regulations to the level of this new data protection culture. In order to improve the business activity environment a balance for the protection of individuals' data and enabling the business activity is needed. In GDPR the motives are mentioned as for example data's movement internationally and for the clearness of legislative improvement: deciders want to grow trust in processing of private data. (Ministry of Finance 2016.)

The regulation also gives the opportunity to dispose a hefty fee for those that do not comply with the GDPR. Hopping & Afifi-Sabet (2019) from ITPRO explains in their article "GDPR fines: How high are they, and how can you avoid them" the two-tiered fining structure of the GDPR: Severe data breaches can be up to €20 million euros or 4% of the annual turnover of the organization, whichever is the highest. And the 2nd lower tier fine is either €10 million, or

2% annual turnover. The organisations are liable to take care of the data security and to prove that the processing is done as securely as possible: the supervising authority has the right to audit the organisations' data security.

The GDPR affects the company's day-to-day routines in every way, except when the company itself is the one who works as the registry, as well as when it's producing services and products, where the personal data is being processed. Suppliers must take into consideration the fact that the safety procedures are even stricter before negotiating any deals, and the companies should be prepared to offer an explanation about their governing and technical data security solutions to their customers. Cybersecurity audits will be done more often.

The job of the data protection officer and proving of the data processing acts are expenses that must be taken into consideration for the company. In Finland, the previous data protection regulation had only a rule of how to uphold registries, but after the GDPR comes into action, the data controller and processors must **document** their processes. Many companies that have taken a serious stance regarding data protection will not have an increased workload when the new regulation is implemented. There will be many companies that have not had the time to prepare for the requirements of the GDPR. In 2018 Gately (2018) reviewed in spring that over 1/3 (around 34%) of the companies located in the United States will not be ready for the GDPR when the transition period is over in May 2018, but they will most probably be compliant towards it by the "latter half of 2018".

The implementation of the GDPR settings requires governing solutions and the improvement of data processing software in the organisations. The implementation of the personal data owner's rights, within the organisation, in a cost efficient way and the birth of the data security standard insist that they are noted in the system. The GDPR demands clear requirements for the data processors' organizations and the part of the documentation process.

2.1 Data subject, Data controller and Data processor

The regulation defines three roles. The regulation is built between these roles' relationship with each other, the rights and responsibilities. The regulation also defines the specific actions of the control officer. Vahti-report (1/2016) defines these roles clearly:

The data subject is a natural person, whose personal data is processed and can be identified within the 'personal data' part. The regulation has special requirements for minors. The minor must be at least 16-years old for the data processing to be legal, but exceptions can be made within the member states of the EU if the age is not less than 13 years.

The data controller is defining the purpose of data processing and its methods. You could even say that the data controller is the supervisor. It is a natural person or legal person, who decides if personal data is going to be processed. The data controller defines the processing basics and methods, and is the main person responsible for the process.

The data processor is an individual that works for the data controllers and handle the data subjects' personal data. The data processor will work with the guidelines created by data controllers. The data processor has a legal responsibility: The processor must make sure that the processing of data is complying with the EUs' or its member states' legal terms.

The data processor can become a data controller if the processor specifies the purpose and methods of the processing of data. A company that processes data must make sure that all its processing methods are singled out in a written agreement. Otherwise, it can surprisingly end up in a more demanding position as a data controller. The process is visualized in the Figure 1.

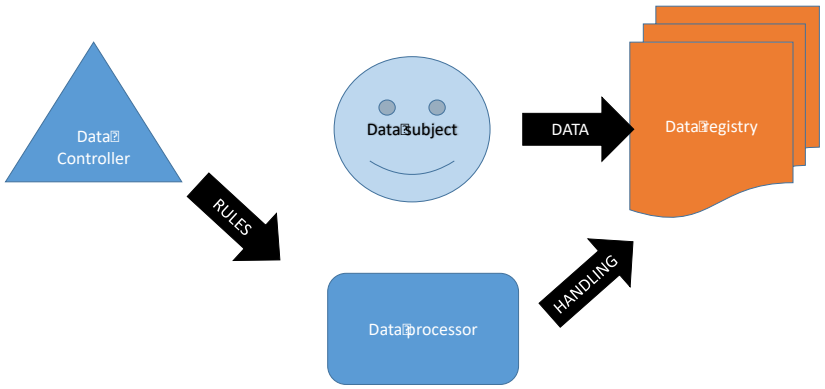

Figure 1 Data handling process

2.2 Personal data and the definition of processing

The data security-regulation only applies to personal data. In the 4th article of the regulation EU 2016/679 this is defined more in detail (EU 2016):

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

It is good to note that when the processing of personal data is ended for any reason, the data can be anonymized rather than being totally erased. This way all the data of the data subject do not necessarily need to be deleted/erased.

Another crucial part of the GDPR is the 'processing'. It is defined in the 4th Article EU 2016/679 the following way (EU 2016):

> *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*

The data processing is about all action that is related to data storing, data modification and data erasure. When personal data has been gathered, the regulation can also limit erasure. The regulations jurisdiction reaches out to, for example, backups, which can cause some interesting things, such as the right of the data subjects to become forgotten.

2.3 Personal Data Lifecycle

The 5th article in EU 2016/679 "Principles relating to processing of personal data" aligns the gathering of data, use and basic rules for preservation (EU 2016). The data controller must define and inform clearly for what purpose the data is collected, so basically it fulfils "the purpose of use". The data is not allowed to be used for other purposes. There is an exception that is formed for statistical and scientific purposes. Gathered information must be limited to the relevant data for the purpose of the use. The regulation calls this "minimizing the data". De la Torre (2019) from The American Bee Journal gives examples of data minimization in her article "What is "data minimization" under EU Data protection Law?". One of the examples uses a debt collection agency collecting debt and searching for a specific debtor. To find the correct person, the search filters the debtors name. Based on the parameters of the debt, all the other data can be removed as it doesn't fulfil "the purpose of use", such as people with the same name and no debt.

As the data processing is ongoing, it is required to keep the data as accurate as possible with reasonable measures or correct errors within the data subject's personal data. The article states that the regulation repeats the requirement for the information to be "whole and confidential" for the safekeeping: Data must be protected from potential misuse and damages.

Personal data is to be deleted, when the data is no longer deemed to be necessary for the data processing. The data can also be anonymized, which means that the data subject can no longer be identified from it. According to the VAHTI-report (1/2016), if the data erasure is being blocked by another regulation, then it must be archived with a necessary method, so that data processing is limited (Ministry of Finance 2016). The report also clarifies that data erasure must be noted somehow so that the data processors do not return to processing for example after a problematic situation such as restoring data from a backup. The regulation calls it as "limiting the storing". For example, in a database, you can attach a token to the Object ID that is not required for the processing. Then when the system receives the backup in this case, then it can be filtered out in a different section.

The data controller has a responsibility to demonstrate these terms, meaning that the controller must prove that these terms are met. It can be done, for example, by drawing up an informational statement. The Informational statement is a free-hand report that strives to offer a whole picture of the data processing in the whole organization: What is being processed, by whom and how.

2.4 The difference compared to the previous regulation

The GDPR replaces the EU-directive 95/46/EY that Finland's current data regulation is based on. The GDPR follows the previous directive mostly, expanding and clarifying its definitions.

Beaumont (2018) from Synopsys writes in her article “The data protection directive versus the GDPR: understanding key changes” about the fundamental differences to the previous directive. The rights of the Data subject are being raised. For example, the right for getting and accessing the data has been improved, as well as the rights of being erased. Although at the same time the foundations have been clarified, for example how the data controller can deny the request of ending the data processing of the subject. GDPR also defines the process of asking consent from the data subject generally and especially from children.

Other new organizational obligations are among others the appointment of the data protector and different data security duties, like data security impact reviews, if for example the data processing has risks. Processors must keep documentation about their processing methods, in case the data subject wants to have clarification how they process the data.

2.5 The rights of the data subject

Protection of the data subject’s information and the individual rights are central within the regulation EU 2016/679 (EU 2016). Personal data processing should always have a lawful basis or the consent of the data subject. The regulation defines carefully in articles 5 to 11 of EU 2016/679 that consent must be asked simply and without pressuring (EU 2016). It is no longer enough to just put a cross in a box at the end of the registration form. If the data subject is under 16 years old, then the consent must be given by the parents. The specific age of majority is determined by each country’s constitution, as long it doesn’t go under the age of 13 years.

The regulation defines multiple ways where the data subjects can gain access to the data concerning the subject itself. The data subject has the right to request their own data and to make necessary corrections to it. The data subject can also demand to transfer the data to another data controller. In other

words, the data must be retrieved in some way, commonly in usable and readable format like for example XML- or JSON-filetypes.

The data subject has also the right to get the data. The VAHTI-report (1/2016) goes through the things that the data controller must inform the data subject (Ministry of Finance 2016). Most of them have already been in the previous data directive, for example the purpose of the registry and the justification of the data processing. The new things are that the data subject must be informed of their rights and the timeframe of how long the data will be kept and offer the contact information of the data controller and how to complain to them. The data controller must also inform the data subject and the authorities about data breaches and other exceptional situations. The data subject must be informed about:

- The purpose of data processing and the personal data groups
- Who has been given the information
- How long the data will be stored and the justification for that
- The data subjects' rights for corrections as well as limiting the data processing and preventing it
- The possible knowledge about automatic decision making and profiling based on the available data of the subject.
- How the rights of the data subject are being protected.
- The origin of the data if the person is someone different than the data subject.

The data subject can also ask that the data processing of their data is terminated. This goes also for correction of data and removal of the data. They can also demand that rather than automatically profiling them, they can request that their data is being processed and the decisions are made by a human.

These rights are not absolute, but the regulation determines different basis to what the data controller can lean on to deny the requests. For example, different legal and fulfilling contract duties or defending both sides legal rights.

2.6 The duties of the data controller.

The data controller is the one who is the main caretaker of the registry and the one responsible on providing the necessary guidelines for the data processors, so that they can uphold the requirements of the GDPR. In the following the thesis will cover the duties and procedures of the Data Controller.

2.6.1 Basis of Law

The data processing is lawful only if there is a defined basis for it in the regulation EU 2016/679 (EU 2016). These definitions are:

- The agreement of the data subject (for example web services)
- Fulfilling the agreement based on the data subject (work contract)
- Statutory obligation (employers' responsibilities)
- Common benefits (epidemical treatment)
- The use of public power/authority
- A natural persons’ protection of their vital rights/benefits (healthcare)

The data subject consent is clearly defined in the regulation. The data controller must be able to prove later that consent has been given and it has been given with the data subjects own free will. For example, during asking the consent from the data subject they need to be informed about the data controllers identity and the purpose of the data processing.

Processing of specifically sensitive data-groups is forbidden per se. These are for example data about race or ethnicity, political and religious views and health. The justice ministry's workgroup, proposed by Nurmi (2017) that insurance companies have the right to process these for working on insurance policies. The processing of these groups needs to have a reason, for example the consent of the data subject, data controllers' fulfilment of their duties and protecting the rights of the data subject. Unions and other similar forces can process their constituents and other key personnel's data, but cannot give out data to others without their consent, within boundaries of the EU 2016/679 (EU 2016).

2.6.2 Privacy by default

The 25th article in EU 2016/679 uses the term "inbuilt and privacy by default" (EU 2016). The data controller must limit the processed data into necessary sections and keep them safe as long it is necessary. The access to the personal data must be limited to only necessary people and the data must not be available to the public.

Privacy by default also means that the data controller must organize technical and administrative procedures to keep data safe. Sensibility is defined by taking into consideration all the available methods and the scope of the process and characterization as well as the risk posed to the data subject.

In principle, the data controller must review the risks of the processing and minimize the amount of the collected data, the scope of the processing and access to the data. As an extra technical method, the personal data can be, for example, hidden or anonymized. Anonymized means that the data subjects' data can be replaced with a temporary identifier so that the personal data cannot be attached directly to the data subject.

2.6.3 Data Security Management

The duties of the data regulation demand that the data security is firmly noted in the business of the entire organization. Depending on the scope of the processing and risks, it means that for example the reviewing of the data processing effects, appointing a data protection officer and constant monitoring of the data protection.

Data Protection Impact Analysis and Privacy Impact Assessments are the regulations' 35th articles enforced procedure. They are important, when the data processing is focusing on sensitive data, if the processing is automatic, if it has legal impact or if there's monitoring an open space for the public, such as the bus terminal for example. "Vahti-report" (1/2016) recommends impact assessments to others as they are a good measure for compliance to the data processing (Ministry of Finance 2016).

Regulation EU 2016/679 defines what parts are required to be included in the assessment (EU 2016). These are especially reviews of the necessity of the data processing methods, risks and methods to counter them. If it is assessed that the risk is high for the processing and there's no way to minimize it, then it is necessary to contact the data protection officer, who will editorialize in the data processing.

There are already multiple governed data protection standards, which adopting to the organisation operations could be good consideration for the protecting of data. In the article "GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance?" by Middleton-Leal (2018) defines a group of recommended procedures, documents and technologies for the governing of the GDPR. Complying with the ISO 27001 requires for example that risk analyses are done in scheduled times, which can execute the GDPR required impact assessments

Data Protection Officer is to be named if a publicly governed facet does data processing, if the processing of personal data is the core of the data controllers' business or if the data processed are especially sensitive or criminal. The

duties of the data protection officer have been defined explicitly in the regulation EU 2016/679; He guides the organization and employees in the complying of the GDPR and doing the impact assessments, governs the compliance of the regulation and collaborates with the data protection officials. He must also be reachable by the data subjects (EU 2016).

The organisation can name a data protection officer, for example, an employee or an external source. It is notable that the data protection officer is aboard in the planning of the data processing from the beginning and he or she does not have conflicts of interest with his other work.

2.6.4 Notification and collaboration

Within the regulation are multiple terms which aim for transparency of the data processing. In the 33rd and 35th article of the EU 2016/679 it is defined as mandatory to inform about data-security violations to the data subject and the data protection officer within 72 hours from noticing the violation (EU 2016). The information must include as much detail as possible: the description of the event and the amount of affected data subjects, contact information of the data protection officer, assessed effects to the data subject and planned actions to minimize the violation.

In the "VAHTI-report" (1/2016) it is estimated that complying with the regulation requires the ability to notice violations/infringements with, for example, software that automatically can analyse log files (Ministry of Finance 2016) . In noticing these it is required sufficient resources and possibly some training. The report recommends that the organizations plan and document as well as the processes of monitoring the information system and reporting, that they prepare beforehand crisis communication by composing message templates and defining the channels which internal and external communication is done by. IT-firms that process data and that offer workstations- and software services can assume that the agreements will include this in the terms in the future.

The 30th article of the EU 2016/679 orders that the data controller must create a description of the processing methods and offer that to the public authority when requested (EU 2016). This can happen for example as a part of 5th article of the EU 2016/679 data processing indication duty execution (EU 2016). The description must have the following information:

- Processing purpose
- Collected data subject groups
- Transference of data
- Moving data to another country and the methods to protect the data
- Description of technical and organizational security methods.

The description is a necessity, if the organization or association have more than 250 employees' or if the processing is reoccurring and if it's defined to cause high risk to the data subject and if data processed is extremely sensitive data subject groups.

Data controller is by the 31st article of the EU 2016/679 required to cooperate with the data security officials (EU 2016). The cooperation can start by the request of the data security officials or, for example, during the effect assessment due to a highly noticed risk causation (change this sentence). The cooperation usually belongs to data controllers' data security responsibilities. "VAHTI-report" (1/2016) also recommends that in the events of a data breach, it is highly recommended to cooperate with the department of communications and the police (Ministry of Finance 2016).

2.6.5 Data transfer outside off Europe

Regulations 44 to 49 article of the EU 2016/679 limits the transferring of data outside of the Europe (EU 2016). Data can be moved without permission to

countries that the EU has deemed to have enough data protection legally and within their government. As of this moment the EU commission has only accepted 12 countries, which the most notable ones are United States of America, Canada and Switzerland.

The data transfer to USA is permitted if the receiving company is part of the Privacy Shield-program. The PS is United States Department of Commerce governed program that companies within its scope are determined to comply its regulations and are legally responsible to comply as well.

Data transfer to other countries is also allowed without consent, if the partners actions/business is protected enough and if the company offers good data protection for the data subject. In practice, this can mean for example that between the data controllers and foreign operators agreements has also involved the European commission approved data regulation statements. The 47th article of EU 2016/679 also enables multinational companies' internal transfers without consent, if the company has compiled specific requirements that fulfils all the department regulations (EU 2016).

On top of the organizations own actions it is good to map out what services and systems move data outside of the EU-borders. Organizations using cloud services for data processing should make sure that it can be determined the geolocation of the cloud service itself. For example, the email- and network drive services could backup information abroad in worst cases.

2.7 Data processor responsibilities

For the personal data processing individuals have been defined demands/requirements in the regulations section article 28 of EU 2016/679 (EU 2016). The basic requirement is that the data processor complies with the defined demands for the data security principles. The data processor always works under the agreement done together with the data controller and is not able to outsource the tasks to a 3rd party without the data controllers consent. The

data processor complies with the data controllers written guidelines, only if they are legally binding. The law can insist the data processor to do such procedures that the data controller has not defined.

The huge part of the data processors requirements comes from the between the data controllers and data processors agreements. The individual taking part in the data processing binds himself to comply to a NDA (Non-Disclosure Agreement). The data processor requires, on top of other processing methods, to collaborate with the data controller for example in making sure that the data subjects rights are kept safe and in the events off a data breach; how to handle the aftermath of it. In the "VAHTI-report" (1/2016) it is recommended that service quality and reporting monitoring are taken into consideration when doing the agreements (Ministry of Finance 2016).

The 30th article in EU 2016/679 states that the data processors upholds documentation of their processing methods (EU 2016). The document includes the same information as the corresponding document from the data controller.

2.8 Agreements and the dividing of duties

The data controller, data processor and other subcontractors' responsibilities are determined deeply into the agreements. The data security-regulation is defined partly on the mandatory parts of the agreement and on their effects. The duties are divided in the following way:

Data controller has the authority to give processing access to the data processor and is responsible of his guidelines lawfulness. Data controller must take care that the data complies with the data security-regulation.

Data processor has the responsibility to comply with the data controllers' guidelines and be assured about their lawfulness. Data processor is responsible for subcontractors' conducts towards the data controllers and data processors' agreement

Subcontractors' position and compensation- and contribution responsibilities are defined according to a contract. So that the subcontractor can be used, it is to be included in the data controllers and data processors contract.

According to the 81st article in EU 2016/679, the damages inflicted upon the data subject can be blamed/put responsibility on as well as the data controllers and the data processors (EU 2016). Data processors is only responsible then, if it has ignored the regulations orders or data controllers' legal guidelines.

Monetary compensation in errors and acts contrary to the regulation can be processed to the data subject. The 83rd article EU 2016/679 determines that the 1st penalty can go up to 10 million € or 2% of the organizations total revenue, whichever is the highest (EU 2016).

2.9 Comparison between the previous directive and GDPR summary

Table 1 presents the things what changes when the GDPR is implemented:

Comparison	**Data protection directive**	**GDPR**
Consent	Businesses' provide a choice for the customer: by adding a box that if ticked, the customer will not receive offers	The details must be specific: • Time limited-opt in, • Must be easily understandable and age appropriate • Requires an opt-out option of profiling
Sanctions	500, 000€ fine, in the case that	Two types of fines: Data Breaches and Admin Breaches. Either up to 4% of annual turnover of the previous year or up to 25 million €

	the data subject got harmed financially	
Notification & Legal Processing	Organizations only required to notify of the data collection	Only after it has been determined that the organization has assessed the data security methods are up-to date and secure enough, can the data controller start processing data subjects' data
Data subject rights	Three rights for a fee: Copy of the data, erasure or rectification of the data.	Same as previously, but without a fee. The organization must provide a portable version of the data, so that the data subject can switch to another provider. And the data subject has the right to know about a Data breach within 72 hours so that they themselves can take necessary steps to protect their own data.
Definition of personal data	Three categories of data that have evolved through the years (change text	Same as previously, except it has widened to include IoT (Internet of Things)
Personal Data Breaches	Non-mandatory to inform	Mandatory to inform
Data Protection officer	Some EU states already have	DPO can be appointed, if the officer doesn't have any conflicts of interests.

	DPO appointment compulsory.	Can be outsourced to external partners if the organization is small.

Table 1 Differences between the DPD and GDPR

3 Audit Process

This chapter will go briefly explain the concepts of the audit, the auditing tool that was used, called “VAHTI” (1/2016), the risk analysis and what are the E-com platforms that are being audited (Ministry of Finance 2016). After the introductions, the work will proceed on the testing and auditing phase of the platforms.

3.1 Audit

Audit is a process that is done on-premises of the target organization to a certain section to inspect and examine that the system that is being audited is compliant towards the GDPR.

There are 3 different types of audits that are suited to specific sections of the organization that is defined by the American Society for Quality (ASQ); Product, Process and System audit. This thesis work is best suited to use the Process and System audit, as the systems that are audited are inspected to confirm the compliance of the GDPR processing of individuals data and that the platforms are prepared for extracting and deleting data. (ASQ 2018.)

There are total of 4 phases to an audit and those are: Preparation, Performance, Reporting and Follow-up and Closure (ASQ 2018):

- In preparation, we confirm the requirements for the audit and what is the end-goal and doing the necessary steps required to ensure the researcher is prepared for the audit. As the Audit starts, the preparation ends.

- Performance summarizes to data-gathering process. It is the beginning of the audit that includes activities surrounding the audit part and the testing phase that is covered in a later chapter.

- Reporting is done after the performance phase is done. This will include informing the participants of the audit and management on the results that were found.

- Last phase is the follow-up and closure. The results from the audit will either prove there is some things that are needed to be added to the systems or either nothing is found and thus ending the audit.

Auditing the preparedness off the organizations compliance towards the GDPR had to be done towards the end of April 2018. The scope of the audit had to be narrowed down to a small section of the organization due to the massiveness of the company and its database resources. It was recommended by the organizations' DPO and E-com IT-manager to narrow down the audit to 2 branches of the company, as they had a prepared a testing environment to test out the compliance. Figure 2 showcases how the project has progressed towards the deadline of 25.5.2018.

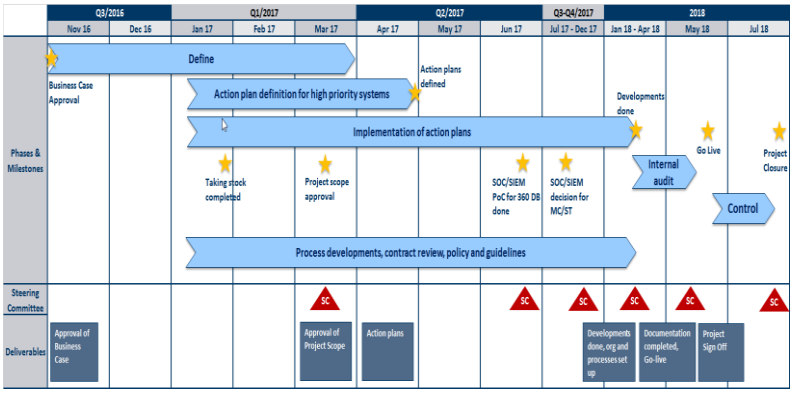

Figure 2 Project Timeline

3.2 Vahti-tool

Ministry of Finance has created an auditing tool in purpose of inspecting and examining the organizations preparedness towards the GDPR, which goes by the name “VAHTI” (1/2016) (Ministry of Finance 2016). The tool is an excel document that covers 3 distinct GDPR topics:

- Data Subjects rights
- Duties of the Data Controller
- Actions

All these steps have different sections within it that relates to that topic, such as the informing the data subject of the data processing reasoning. It also has section where it is covered the analysing section of the present situation. It is either Recognized, 25%, 50%, 75% or 100% ready. After choosing one of those options, the document calculates a number to represent the score of the audit process of the test that is being conducted. Main focuses of this tool that is used in the test are as following:

- Data controllers informing duty
- The right to gain access to personal data
- The right to correct data
- The right to erase data (“right to be forgotten”)
- The right to change data from a system to another
- The right to deny the automatic profiling of the data subject
- The right to get information from data breaches.

3.3 Information classification and the team.

What information classification means in this case, is that how relevant and important the data is for the organisation in this setting. Due to the testing focusing on E-commerce of the organisations 2 branches, it must be defined what data is required from the data subject, how to classify the data correctly and who can see data subjects' information. As this gets clarified, the organisation achieves better understanding off their data handling processes. Due to the focus of the audit being on E-commerce only, the physical data material won't be included in it.

The case organisation has implemented monitoring systems for electronic material and how the classification practices are followed. This is handled by a team that was formed for the GDPR. The IT-manager works as the Data Controller for the team and the data processors follow his guidelines. The team members have all went through an E-learning course within the organization, which can be found in the organizations own intranet. This ensures that the data processors within the team are fully capable of handling sensitive data and what to do in situations covered in the regulation, such as data breaches. As for the data classification, in this environment the data handled is classified as personal data (name, birthday) and not as sensitive data (ethnicity, religion), due to the requested information when creating an account are only the following:

1. First & Last Name
2. E-mail address
3. Birthday
4. Password

There are more data that can be added to the account, but the information mentioned previously are the ones that are mandatory for the creation of an account.

The interview that was conducted gave insight about the processing methods of the team that covers the GDPR-compliance. The preparedness of the whole team is compliant towards the GDPR and they have the necessary skillset on tackling GDPR-related topics. To note is that there are guidelines that can be found on the organizations intranet to refresh the memory of every employee in the organization that what is covered in the regulation.

Recommendations: Review after a period the knowledge of the team and how the process has been going forward with handling data classification.

3.4 Testing of creating an account

There are 2 branches that are participating in this audit test, so there will be total of 2 tests done for each platform. These are using the same database, though they store the data subjects' data in different sections. The test will also cover, if the data is getting properly transferred to the correct location.

These E-com platforms are Electronic Commerce Platforms. Article "What is ecommerce?" from Markus (2019) explains that they are platforms that provide an online front for conducting transactions with the target organization. As you are buying or selling something through the internet, you are part of an ecommerce transaction.

There are numerous different classifications for ecommerce platforms, such as:

- Ecommerce stores that sell physical goods
- Main business is service-oriented. Examples are consultations or educators.
- Digital Products selling platforms. For example, Steam sells games through their own platform.

The target organization platforms are selling physical goods to their customers as Business to Customer (B2C). The items sold in these platforms are showcased online and the customer using these platforms can add the items they want in to a virtual cart that they can "push to the checkout". After the necessary monetary transactions are done, the organization will use the details provided by the customer, when they've created an account to the page, to ship the items to the correct destination or to pick up from the organizations stores within proximity of the customer.

The platforms are a storefront for the organization and they are the most viable solution for straightforward ecommerce. When interviewing the owner of these platforms, one fundamental question needed an answer:

- What is the platform technology based on?
- What technologies it uses?
- How is the data protected?
- What is done in the event of a data subject requesting that their data is not automatically profiled?
- What is done in the event of a data breach?

To answer the questions, they are based on ecommerce service platform provided by Magento. As specified by Lodge (2019) in her article "What is Magento?", Magento provides flexibility and an extension of functionalities to freely modify the storefront to look exactly how the organization wants to.

How the GDPR provides data protection to these platforms, the team implemented security measures for the accounts created on the platforms. The systems are using PHP (Scripting language for web developing) and MySQL (database management system). As the accounts are created to the database, MySQL encrypts the data that the customer provides, such as their password and user-id.

If the customer requests that their data is not automatically profiled by the systems implemented by the organization, then the data subject will have a token attached to their account in the back end of the database, grouping them with other similar individuals that do not want automatic profiling. There will be then people working on their data if they have requests.

In the event of a data breach, the security team within the organization will for the 1st step minimize the impact as much as possible. As all the users have to have e-mail addresses within their accounts, the team can send a mass message to everyone involved that a data breach has happened.

The test will include the following sections:

1. Creating a dummy-user in the E-com platform
2. Customizing the settings with adding profile data
3. Logging out and in to synchronize the changes within the DB
4. Changing personal data in the profile
5. Requesting that all data is moved for export (for example, xlsx. (Data portability)
6. Verifying that all the data has been removed the database
7. Verifying that all the data has been removed from the E-com platform

The test was done in a testing environment provided by the team in France. Hence the pictures are in French. Note that the usernames, data sensitive to the company and mentions about the portal name has been erased, as the request for this thesis was not to mention the organizations name.

3.4.1 Test

The 1st part of the test covers the creating of the account to the 1st platform. After the initial part is done, adding data for the account such as first- and last name, an e-mail was sent to the corresponding team making sure that the creation of the account has been successful, as seen in Figure 3.

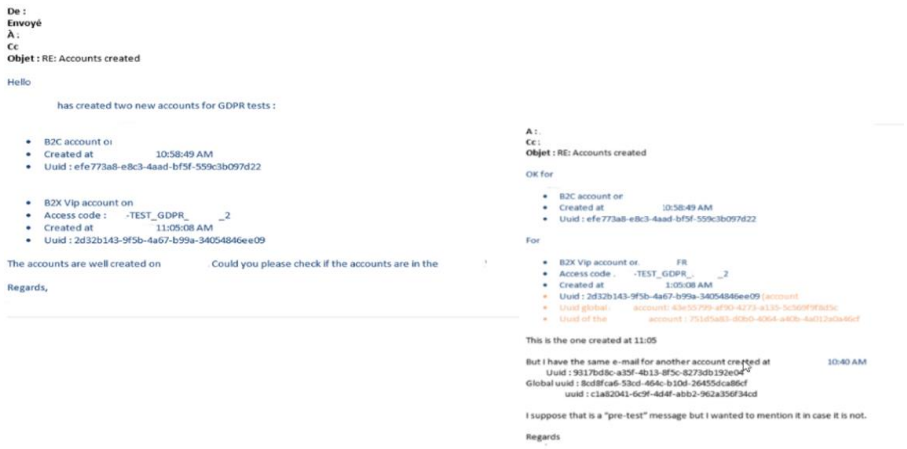

Figure 3 Account creation

2nd part of the test is covering about customizing the account by adding personal data to it. In this section, there can only be added first- and last name, e-mail address, date of birth and password. There's also a possibility to subscribe to newsletters that include 7 different sporting categories within this specific brand and accepting the terms and conditions for this. The terms and conditions are seen in Figure 4:

1. Summary of the GDPR
2. What data is being collected
3. The purpose what the data is used for

4. Personal data transferring & Underage data
5. Correctness of the data (up-to-date)
6. Data security
7. The rights of the data subject & contact information

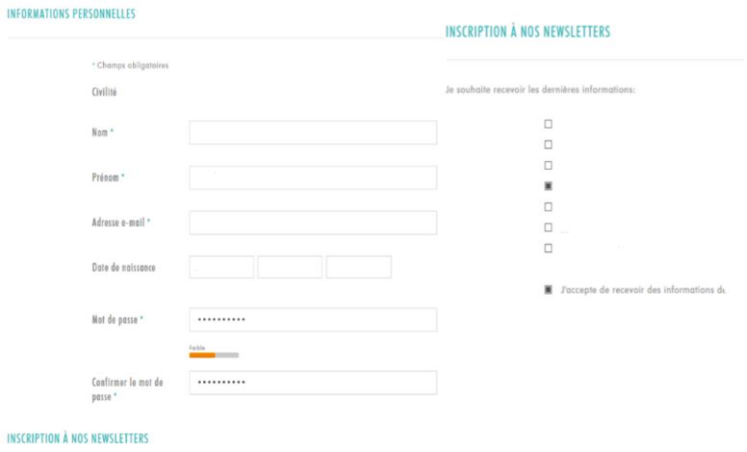

Figure 4 Adding data

Continuing with adding data, the next section expands on the information of the data owner, where the account owner can add his/her home address, postal code, city, country and telephone number. There's also a possibility to choose the address provided as the main place when ordering items online. After the data has been given, you can see the changes on the new window. This is visualized in the Figure 5.

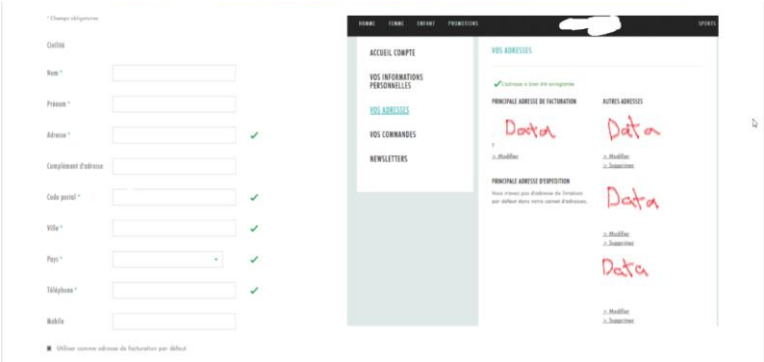

Figure 5 Customizing data

Now that the account has been created and personal data added to it, we'll confirm from the team responsible of handling the data that the changes are visible within the database. For the data to get synchronized within the database, it is required to log-out and logging back in to the e-com portal. The initial test did not work as intended and the data wasn't updated to the platform.

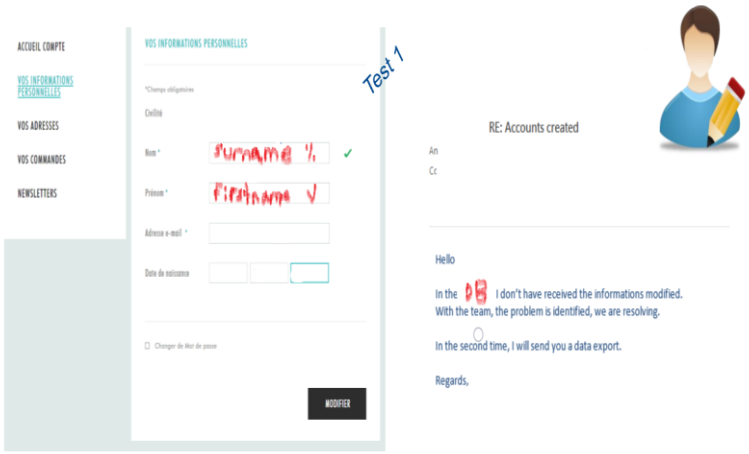

Figure 6 Changing data

Due to the data synchronization not working properly, as confirmed in the email in Figure 6, a re-test was done a week later by changing the name of accounts first-and last name. The previously mentioned synchronization issue was corrected, and the data was now visible within the database. The team provided the account information in PDF-format as it can be seen in the Figure 7.

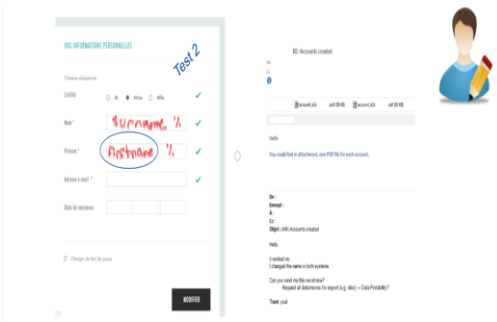

Figure 7 Changing data 2

For the 5th step is to test out the data portability. In the event where the data subject wants to change the data registry and the data controller of their data, the data subject can request that all the available data is ported to XLS, JSON or PDF format. In this case the ported data is exported in XML format, which is similar and functions the same way as XLS format with few alterations (XML is the newer version of the XLS, which are Excel-formats). This is covered in the Figure 8.

Figure 8 Data portability

6th step covers the part where every ounce of data is removed & deleted from the organizations database. This is one of the main topics covered within the GDPR, where the data owner can dictate the use of his own data and request the deletion of everything from the case organizations database. If not complied, the organization can face up to 4% of total turnover or 25 million €, or whichever is the highest, of sanctions.

Figure 9 Data deletion

The final part of the test was to confirm that the data and accounts are completely removed from the database, as can be seen in the Figure 9. To confirm that the account was removed, another test was completed similar way with similar e-mail address. Due to no duplicate accounts aren't allowed within the database, the test was successful. This was also confirmed by email, which can be seen in the Figure 10.

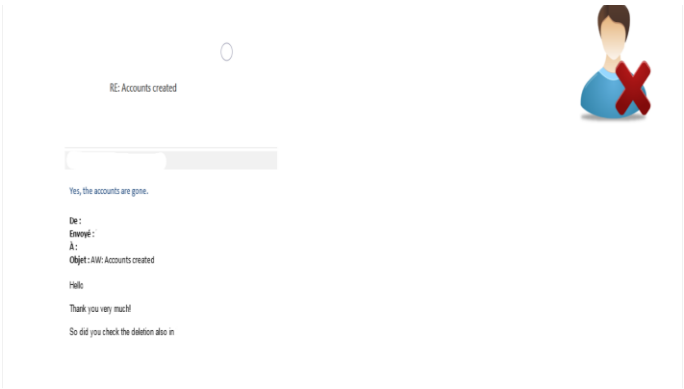

Figure 10 Confirmation of data deletion

The account creation was a successful with few hiccups in the beginning with the synchronization with the data. This was quickly corrected after sending message forward to the team and after that the synchronization worked.

Something to note during this test was that the page didn't have a finalized version of the Terms and Agreements of the GDPR, but after re-checking this, the account creation section had included the reviewing of the GDPR-statement of the organization. This can be also found within the footer of the webpage, clarifying the contact information of the organization on who to contact with inquiry about data subjects' own data and as well as legal requirements of the organization.

Overall the compliance of these two e-com portals are on a level that is acceptable within the scope of the GDPR and can be fully implemented. However, it must be taken into consideration that human error can happen, which can have negative impact on the organization.

4 Results

According to the auditing and testing of the organization, it's clear that they are not in any immediate threat from outside or the inside and that the compliance of the platforms are GDPR-compliant. Noteworthy mentions in the test was that there was missing from the platforms is the informing of the data subjects' rights or the GDPR-statement of the company. This was corrected after the researcher noted this to the correct personnel and after the 2nd test it was added to the platforms.

Before beginning the test, we needed to identify the questions that needed to be answered through the test. Table 2, Parameters of the test show the results from the tests:

Table 2 Parameters of the test

Parameters	**Compliance status**
1.Data controllers informing duty	100%
2. The right to gain access to personal data	100%
3.The right to correct data	100%
4.The right to erase data ("right to be forgotten")	100%
5.The right to change data from a system to another	100%
6.The right to deny the automatic profiling of the data subject	100%
7.The right to get information from data breaches.	100%.

As the test for these e-com platforms were done, it was noted that they were missing the GDPR statement of the organization on how and what data they process, including the rights of the data subject. After informing about this to the platform owners, the 2nd test that was inducted showed that they had implemented it when creating a new account.

The access to the data subjects own personal data was tested by logging into the account of the platform. From account-management the data was visible for the data subject. This was also confirmed through e-mail from one of the data processors of these platforms. During the same time, the researcher tested out the data modification of the account and was able to do that. This was also confirmed through email.

As for the data erasure, it was tested 2 times. After the 1st test, the researcher sent a message to the owner of the platform, requesting to delete all data for the specified account that was created. To confirm that the data was deleted, another account was created with identical data. It was a success, meaning that the data erasure was done for the account. To clarify, the system behind the E-com platform does not allow duplicate accounts within the database.

Testing the functionality of the data portability was successful as well. By sending an e-mail to the platform owners, the researcher requested for the data to be packed up so that the data can be ported to another database. The processors behind the platform sent an XML-file with all the account data for this specified account. The other database was used for the 2nd test, where the researcher requested the data to be forwarded.

As for the automatic profiling, this was asked through the interview from the platform owner on how they do it. If the customer requests that a human works on their data and not an automatic entity, then they will be attached with a token that groups people together in the database that do not want their data to be automatically profiled.

Last, but not least, the data breaches. In the event of a data breach happening, the security team within the organization works together with the e-com platform owners if they are impacted anyhow. As all the accounts require an email address, the database can be used to send a mass message to all the users in the event this happens.

5 Conclusions

These platforms were tested twice. As the requirement for the platforms to be compliant with GDPR must be 100%, the test was deemed a failure if for example data erasure did not erase everything.

The 1st test was conducted, and as it was missing the GDPR statement of the organization, the test was deemed to be a failure. The 2nd test had the statement added to it and all the other parameters were set that were defined in Table 2 before starting of the tests. The test was 100% successful. The success ratio of these two tests is then 50%.

The main finding of these tests was to visualize the complexity of these platforms. Numerous things need to be taken into consideration when making the platform compliant with GDPR. As these platforms are now prepared for the GDPR, they can be used as templates for future platforms that include the same parameters set in these tests.

At the start of this thesis, work the researcher set up the following aims:

- Finding missing parts from the audit
- Create platforms compliant with GDPR
- Understanding the GDPR.

The audit revealed missing sections that are requirements for the compliance of the new regulation. These were corrected by the request of the researcher, making the platforms compliant.

The research journey also gave more insights about the new regulation and its influence on the day-to-day work in normal settings within the organisation. This will be beneficial for the future development of GDPR compatibility. It is always advantageous to have thorough understanding about legal issues in data handling processes.

References

Electronic sources

American Society for Quality. 2018. What is Auditing? Accessed 15 October 2018 http://asq.org/learn-about-quality/auditing/

Beaumont. S. 2018. The data protection directive versus the GDPR: understanding key changes. Accessed 13 April 2018. https://gdpr.report/news/2018/03/06/data-protection-directive-versus-gdpr-understanding-key-changes/

De la Torre. L. 2019. What is "data minimization" under EU Data Protection Law? Accessed 21 May 2019. https://medium.com/golden-data/what-is-data-minimization-under-eu-data-protection-law-b0e30fbb856e

European Union. 2016. General Data Protection Regulation 2016/679. Chapter 1-89. Accessed 15 January 2018 – 3 June 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Gately. E. 2018. 1 in 3 Companies Not Ready for GDPR Compliance. Accessed 13 April 2018. https://www.channelpartnersonline.com/2018/04/02/1-in-3-companies-not-ready-for-gdpr-compliance/

Hopping. C. & Afifi-Sabet. K. 2019. GDPR fines: How high are they, and how can you avoid them? Accessed 15 May 2019. https://www.itpro.co.uk/general-data-protection-regulation-gdpr/31025/gdpr-fines-how-high-are-they-and-how-can-you-avoid

Lodge. K. What is magento? Accessed 21 May 2019. https://www.commonplaces.com/blog/what-is-magento/

Markus. J. 2019. What is ecommerce? Accessed 21 May 2019. https://www.oberlo.com/ecommerce-wiki/ecommerce

Middleton-Lean. M. 2018. GDPR and ISO 27001 Mapping: Is ISO 27001 Enough for GDPR Compliance? Accessed 21 May 2019. https://blog.netwrix.com/2018/04/26/gdpr-and-iso-27001-mapping-is-iso-27001-enough-for-gdpr-compliance/

Ministry of Finance. 2016. EU-tietosuojan kokonaisuudistus, VAHTI-raportti – 1/2016. Accessed 15 January 2018- 3 June 2018. https://www.vahtio-hje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Nurmi. P. 2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö. Acccessed 14 April 2018. http://julkaisut.valtioneu-vosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tieto-suoja.pdf?sequence=1&isAllowed=y

Figures

Figure 1 Data handling process 10

Figure 3 Project Timeline 25

Figure 4 Account creation 31

Figure 5 Adding data 32

Figure 6 Customizing data 33

Figure 7 Changing data 33

Figure 8 Changing data 2 34

Figure 9 Data portability 35

Figure 10 Data deletion 36

Figure 11 Confirmation of data deletion 37

Tables

Table 1 Differences between the DPD and GDPR 24

Table 2 Parameters of the test 38

Appendices

Appendix 1: First appendix..... **Virhe. Kirjanmerkkiä ei ole määritetty.**