Haaga-Helia
University of Applied Sciences

GDPR – Six Months After the D-Day

Iiro Lehtisalo

Master's Thesis
Degree Programme in Information Systems Management
2018

Haaga-Helia
University of Applied Sciences

Abstract

19.11.2018

Author
Iiro Lehtisalo

Degree programme in Information Systems Management, Master's Degree

Report/thesis title	**Number of pages and appendix pages**
GDPR – Six Months After the D-Day	**39 + 3**

The General Data Protection Regulation passed 2016 and the regulation was enforced on May 2018. The regulation aims to protect personal data, that are controlled and processed by companies and organisations.

Due to the Regulation, natural persons may request companies to provide all information they have regarding the data subject. Natural persons also request companies to correct the information, to withdraw their consent on using the data or to request to erase the data and forget them.

For companies the GDPR brought an obligation of accountability, reporting the security breaches, and possibility of sanctions. For natural persons the GDPR brought transparency on, how their personal information is controlled and processed by the companies.

The GDPR still evolves, because many EU member states are harmonising their legislation to comply with the Regulation. In Finland, the national law passed 13th November 2018. New ways of mass processing information, like Artificial Intelligence, need to consider the GDPR restrictions in their development.

My goal was to discover in what ways the GDPR has presented itself to companies and to natural persons. I reviewed the GDPR main concepts in the theoretical part of this thesis. I continue from theory to review the financial impact and first six months events after the enforcement. I interviewed data privacy experts to understand the company's point of view on GDPR and to understand, what they have done to comply with the Regulation. Finally, I present self-probing results, where I have exercised my right to access my personal data the selected companies control and process.

The GDPR has been a tough project for companies. On average 12 to 18 months lasting, involving tens of people around the company and outside the company. The cost and the extent of the project has asked a lot of resources; thus, a lot of companies have seen the whole project as a nuisance.

Companies have not realised the size of the project fully, when engaging with their GDPR projects. This has led the focus solely on information systems and overwhelming hassle. Focus on information systems has diminished the focus on companies' business processes.

Based on my self-experimental probing, the companies collect, and control data based on their business needs and comparison between the companies is difficult even, if the core business is the same.

Keywords
GDPR, Data Privacy, Right to Access

Table of contents

1 Introduction ... 1
1.1 Objectives and Research Questions ... 2
2 GDPR in general ... 4
2.1 Territorial Scope ... 5
2.2 Personal Data ... 5
2.3 Right to be Forgotten ... 6
2.4 Breach Notification ... 6
2.5 Right to Access ... 7
2.6 Data Portability ... 7
2.7 Privacy by Design ... 8
2.8 Data Protection Officers ... 8
2.9 Consent ... 8
2.10 Data Protection Impact Analysis (DPIA) ... 9
2.11 Fines and Penalties ... 9
2.12 Accountability ... 10
2.13 GDPR and Artificial Intelligence (AI) ... 10
3 Methodology ... 12
4 What Has Happened Since Enforcement Of GDPR ... 14
4.1 Economic Impact of GDPR To Companies ... 14
4.2 Court Cases Concerning Data Privacy ... 17
5 Empirical Results – interview and testing in real life ... 19
5.1 Data Privacy expert Interview Results ... 19
5.2 Data Privacy expert Interview Analysis ... 26
5.3 Self-probing Cumulative Results ... 30
5.4 Self-probing cumulative Analysis ... 32
6 Conclusion ... 34
References ... 36
Appendices ... 40
Appendix 1. Disclosed GDPR Report Consumer Retail Company A part 1 ... 40
Appendix 2. Disclosed GDPR Report Consumer Retail Company A part 2 ... 40
Appendix 3. Disclosed GDPR Report Consumer Retail Company A part 3 ... 40
Appendix 4. Disclosed GDPR Report Consumer Retail Company A part 4 ... 40
Appendix 5. Disclosed GDPR Report Consumer Retail Company A part 5 ... 40
Appendix 6. Disclosed GDPR Report Consumer Retail Company A part 6 ... 40
Appendix 7. Disclosed GDPR Report Consumer Retail Company B ... 40
Appendix 8. Disclosed GDPR Report Transportation Company ... 40
Appendix 9. Miten Suomessa ohjeistetaan pieniä yrityksiä toimimaan? ... 41

1 Introduction

The GDPR or more officially The General Data Protection Regulation (2016/679) was enforced on 25th of May 2018. Before the enforcement date, the data privacy and data protection have been hot discussion topics in Europe for past couple of years. All companies doing business in EU area are affected by the scope of GDPR as all companies control or process personal data of their customers or at least their employees.

The regulation harmonises data protection legislation within the European Union, thus companies cannot change their location to other countries, where data privacy violations would have smaller sanctions.

Like all upcoming regulative acts, there is lot of debates and even confusion regarding the appropriate measures to be taken in order fulfil the obligations. As expectable, there has been several companies sharing their knowledge and opinions, what to take into account during the GDPR project. There is no right answer, how companies should get compliant and therefore we have seen over- and underreactions.

As the intensity of private data processing varies from business to business, so does their readiness to adapt the new data protection regulation. The actual measures that companies have done to comply with GDPR have therefore been different from each other.

Although the GDPR was enforced six months before this thesis, several experts have an opinion that every organisation have still a lot to do regarding their data privacy. For those small companies, who still doubt their GDPR readiness, I have addressed a checklist in the appendix of this Thesis.

GDPR compliance is still on top of several company's agenda. The national data protection law in Finland passed on 13th November 2018. Before the law passed, the National Data Protection Ombudsman could not give sanctions to companies, who violated the GDPR.

The GDPR and data protection in general is expected to slow down the utilisation of data in its mass processing applications, like AI and automated decision-making. All companies, who intend to utilise machine learning, need to understand the GDPR restrictions in their actions. In near future we will find out, how data protection and data mass utilisation can live together.

I intend to take a look into the key concepts of the GDPR, that all companies should understand. Further on I interview an GDPR expert company, who has been helping their customers in data privacy projects. Lastly, I test, how the GDPR works for a natural person, for whom the GDPR has been made, and evaluate, how the “Right to Access” work in reality.

The scope of Thesis in Finnish companies. The regulation applies to all companies and organisations, private and public. Due to large amount of companies in Finland, I found most interesting to study, how such heterogenous group has adapted the new regulation.

The thesis was ordered by Haaga-Helia University of Applied Sciences.

1.1 Objectives and Research Questions

My objective is understanding the essence of the GDPR and to help natural persons and companies to understand their rights and responsibilities. The GDPR gives the data ownership back to data subjects and obliges the companies to treasure the data they control and possess.

The purpose of this work and my interest is to study and to answer the following questions:

1) What are the main concepts of GDPR?
2) What has really happened? What are the first wave actions we have seen since 25th of May 2018?
3) What does the GDPR really mean for companies and for natural persons?

Data Privacy in general is getting even more interesting and complicated the further the digital services develop, and companies start to utilize AI. To work and to develop, the machine learning needs data and the GDPR restricts the use of data greatly. Natural persons have given their private information and companies as well as public sector organisations and they have collected the private data often without thorough justification, why the information is collected. The objective of GDPR was to regulate, how this information is controlled and processed.

My first research question aims to discover the main concepts of the regulation and explain, what rights natural persons have, and what obligations the organisations need to comply with.

Several different companies started their marketing campaign roughly two years before enforcement day of GDPR and the pace of public speaks increased as the GDPR date became closer. While there has been a lot of talking about the GDPR, I have been wondering, what the companies have really done to comply with the Regulation. Has the compliance project been mainly about IT systems or have companies looked into their business processes, which may need the private data to run? I also want to look into the news streams and to find what legislative measures, if any, have been taken since the end of May 2018 regarding GDPR.

Without a doubt, new obligations of GDPR have pushed companies to take certain actions but, perhaps, more importantly individuals have more privileges. Anyone can ask to see the information any organisation controls about them and also decide, if they can keep doing so. My third research question brings the GDPR to grass root level and see, what kind of information we can ask to see from different companies.

2 GDPR in general

In this chapter I take a short overview on the General Data Protection Regulation. My aim is to choose the main points of the history of the Regulation and illustrate the journey, how the GDPR was born.

European Union passed first Directive concerning data protection in 1995. Officially the Directive was called “Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (EUR-lex, 2018). This Directive received several revisions and additions during the years, as illustrated in Figure 1, until 25th of May 2018, when GDPR entered into force.

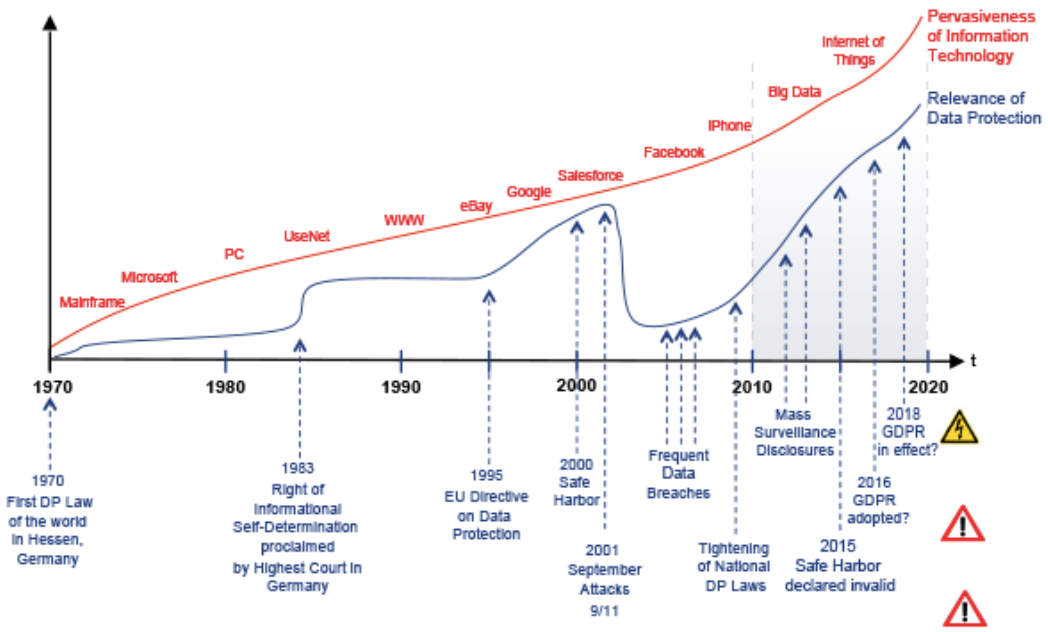

Figure1. A brief history of General Data Protection Regulation

The difference between the previous directives and current regulation is that by a definition: “A regulation is a binding legislative act. It must be applied in its entirety across the EU”, while “A directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals” (European Data Protection Supervisor, 2018).

The previous directives were also considerably narrower by its field of application and environment has changed dramatically since the dawn of internet. EU Commission’s aim was to strengthen the online privacy and accelerate digital economy within EU area (European Data Protection Supervisor, 2018). Personal data is one of the key concepts in GDPR and I intend to take closer look to it in chapter 2.1.

GDPR has indeed been a substantial effort from legislator's and organisations' point of view. It is also important to notice that the GDPR is not the end of legislative work around data privacy in European Union. Currently the next regulation proposal called ePrivacy is in process, but its approval and enforcement dates are not yet published. Interestingly the GDPR has worked as a benchmark for initiatives globally to enforce the personal data protection legislation.

2.1 Territorial Scope

The General Data Protection Regulation (2016/679) covers all natural persons residing in EU area regardless of the companies' location controlling the data. In other words, all companies in EU area and outside EU area processing EU citizens' personal information must comply with the regulation.

2.2 Personal Data

Cornerstone of the GDPR is personal data. What it is and how it should be handled are the key questions, that companies should consider. Article 5 sets principles of personal data processing. Because of the importance of the subject, it is good to take deeper look into Article 5. According to it personal data should be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner, that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The controller is responsible for and able to demonstrate compliance with the above-mentioned principles. The article 5 contains several key principles of the regulations, that several companies have included in their GDPR guides.

GDPR sets a wider scope to personal data, than previous legislation. Article 4 defines it as: “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.”

Description is very broad, and it covers a wide array of different identifiers. Examples of such identifiers are cookies on web-sites, MAC and IP-addresses, social media postings, and other individual identifiers, which, together with other, help to identify a natural person.

2.3 Right to be Forgotten

The data subject may ask data controller to erase personal data concerning him or her and the data controller must act accordingly without undue delay, unless one of the following reasons applies:

1) personal data is still necessary for the processor for the reasons it was collected;
2) data subject consent withdrawal has no legal ground;
3) personal data is lawfully processed;
4) no Member State or Union law conflicts with keeping it saved;
5) the personal data is not about child under 16.

The meaning of the above is that a natural person may ask any processor to wipe the information they have gathered on him or her, if there are no legal grounds of having it. There are some questions open and yet to be defined, when the mentioned legal grounds are no longer valid, such as private vs. public interest.

2.4 Breach Notification

Article 33 states, that the controller shall give a notice to supervisory authority within 72 hours of becoming aware of personal data breach. In case the notice is not given within 72 hours, there should be acceptable explanation. The notice should describe the nature

and the magnitude of data breach, contact details of company's DPO, consequences of the breach, measures taken and intended to be taken to mitigate the consequences.

2.5 Right to Access

Right of Access for data subjects to their data is without a doubt one of the most important and one of the most discussed subjects in GDPR for several reasons: it can be laborious for data controllers or processors to perform, and on other hand it opens the door for data subjects to further exercise their rights to rectify the information collected from them or discover possibly wrong information or inadequate disclosure of their data.

Once the request is placed to processor, they must within a month give a thorough report about the data they process or control regarding the data subject. The report should contain following dimensions:

a) processing purposes,
b) categories of data,
c) recipients or category of recipients,
d) planned duration of storage,
e) information about data subject's rights (erasure, rectification, restrictions),
f) instructions, how to file a complaint to authorities,
g) information about data origin,
h) existence of any algorithm-based processing of the data and consequences of such procedures,
i) possible distribution of personal data to external parties or countries without appropriate level of data protection.

The report is to be given once free of charge electrically or verbally if applicable. In case the controller has large quantities of data of the subject, they may ask to specify the request to certain categories or types of information.

2.6 Data Portability

A data subject or natural person may ask the data controller to hand over all data, the data subject has provided, in machine-readable and commonly used format. The data subject has a right to transmit that data to another controller without hindrance of previous data controller. Where technically feasible, the previous and the new controller should transmit the data between them.

This means that data controller does not own the data of their customers, but the data ownership is shifted to data subjects. This change enables natural persons to change their

service vendors (e.g. insurance, banks) and possibly get benefits from their immaculate history.

2.7 Privacy by Design

Privacy by Design in one of the cornerstone concepts of GDPR. By Ann Cavoukian, the principles are:

1) proactive not reactive; preventive not remedial;
2) privacy as the default setting;
3) privacy embedded into design;
4) full functionality; positive-sum; not zero-sum;
5) end-to-end security: full lifecycle protection;
6) visibility and transparency: keep it open;
7) respect for user privacy: keep it user-centric.

Privacy by Design covers IT-systems, accountable business practices and networked infrastructure (Cavoukian, 2018). The principles defined in 90's have prevailed and became a widely acknowledged standard for data privacy legislations around the world. As the privacy by design concept prerequisite is minimal data processing, some companies might need to consider the business applications they use and how they use them.

2.8 Data Protection Officers

The GDPR introduced the concept of Data Protection Officer. Both data controller and data processor shall designate a DPO either from their own staff, or hire a contractor to fulfil the obligation. Not all companies need the DPO, only public authorities need to have one, but private companies need to appoint one in following cases:

a) the core activities of controller or processor require regular and systematic monitoring of data subjects in large scale; or
b) the core activities of controller or processor consist of processing large scale of special categories of natural persons, such as political opinions, criminal records, ethnic origin, religion, sexual life or orientation.

The main duties of DPO are to be a contact person for supervisory authorities, inform, train and advice the data controller and processor and their employees, and monitor the compliance with the GDPR.

2.9 Consent

As important as processing the personal data in an appropriate manner is that the processor has a right to do so. For this the processor must have the consent of the data subject.

The article 6 Of GDPR states that in general processing personal data is prohibited, unless it is expressly allowed by the law, or data subject has consented to the processing. The consent should be given by free choice, it should be specific, informed and unambiguous. This means that a data subject (person) can choose not to give consent without a risk to have negative consequences. A recommended way to give a consent is to make an opt-in action, in written or in electronic form.

A consent should be as easy to cancel as it is to give. This can be challenging for several companies, which use personal information for large campaigns, or which keep their customer's information in several different location.

2.10 Data Protection Impact Analysis (DPIA)

Companies who process sensitive personal data of natural persons must analyse their data processing processes on regular basis – at least every three years. The assessment should consider the technology and processes where the personal data flows. DPIA exercise must be performed especially when company is adapting new technologies to ensure their compliance regarding the Regulation.

2.11 Fines and Penalties

The maximum penalties for companies have been one of the biggest changes compared to previous directive as well as the substantial size of the penalty – 20M€ or 4% of company's global turnover, whichever is higher. This has, for a good reason, drawn attention of the companies to GDPR. However, the mentioned figures are the maximum penalty and no such penalties have so far been given.

Before such penalties can be given, national authorities can give several minor penalties such as order corrective measures, where violations are noticed, or impose temporary or definitive ban of processing personal data. The penalties follow the severity of the violation and the level cooperation of a violator. The national data protection law passed on 13th of November 2018 (Eduskunta, 2018) and by the time of this thesis there are not yet any court decision in Finland.

2.12 Accountability

All data controllers must be ready present its compliance in private data processing. According to the Office of Data Protection Ombudsman, the following measures and documents prove the implementation of accountability (Office of Data Protection Ombudsman, 2018):

- A record of processing activities, i.e. a general description of the processing of personal data (GDPR, Article 30)
  - This also applies to processors of personal data
- The realisation of data protection by design and by default in operations (Articles 5 and 25)
- Possible wider data protection policies (Article 24.2)
- Notification practices (Articles 12–14)
- Evaluations of the legal basis for processing (Articles 6–10)
  - If the processing is based on consent, the documentation related to consent (Articles 7 and 8)
  - If the processing is based on the legitimate interests of the controller or a third party, the balance test (Article 6.1.f)
- Other internal and external guidelines (Articles 12, 13, 14, 24, 25, 28, 29 and 32)
  - The risk assessment documentation and technical and organisational safeguards implemented
  - Internal and external guidelines for exercising the rights of the data subjects
  - Instructions for processors and personnel who process personal data
  - Internal inspections and audits
- Impact assessment (Article 35) and prior consultation (Article 36) documentation
- Documentation of personal data breaches (Articles 33 and 34) and the related process
- Documentation related to the position and duties of the Data Protection Officer (Articles 37–39)
  - If the organisation decides to adopt a solution not advised by the Data Protection Officer for processing personal data, the grounds for the decision should always be documented
- Agreements related to the processing of personal data (Article 28)
- Areas of responsibility of joint controllers (Article 29)
- Possible documentation concerning the definition of the lead supervisory authority (Article 56)
- Documentation on the transfer of personal data to third countries (Chapter V)

Although it may seem like a lot of documents, not all companies need to have all of them. However, if a company chooses not to make any of these, the decision and its reasons should be documented.

2.13 GDPR and Artificial Intelligence (AI)

Artificial Intelligence is without a doubt a field of technology we will witness to grow in near future. AI is even expected to replace certain professions, when it is developed. To improve and to develop the AI needs large amount of data, which is frequently subject to GDPR requirements. The Article 22, with headline “Automated individual decision making,

including profiling" explains, how the GDPR restrains the private data in machine learning applications:

1) "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

2) "Paragraph 1 shall not apply if the decision: is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent."

3) "In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

As we can see, the regulation does not explicitly forbid the use of private data in automated decision-making applications but constrains it. Even experts have not found a common view, how the GDPR can live together. On the other hand, GDPR restricts the personal data by purpose limitation, consent, storage limitation, and data minimisation. And on the other hand, if the paragraph one doesn't apply, there should not be a problem.

Companies are also obliged to explain the data subject, how and why automated decision-making application came to certain conclusion regarding the data subject. The broadness of definition leaves a room for interpretation and first court cases will eventually tell us, how the Regulation should be understood.

The SAS Institute interviewed companies globally during the spring 2018. According to their report, 49% of the companies said, that "GDPR will significantly impact their AI projects" (SAS, 2018). According to this research, the companies mentioned as most concerning issues establishing informed consent, logging/presenting to auditors details on use of profiling, and requiring human involvement on AI decisions.

3 Methodology

The method of my study is qualitative analysis. By this practical approach my goal is to find out, what companies have actually done regarding the GDPR, and how the new regulation is implemented in regular companies. Although the data privacy regulation's objective is to protect the natural person's data, the most changes will be done by organisations.

My research questions are:

1) What are the main concepts of GDPR?
2) What has really happened? What are first wave actions we have seen since May 25th, 2018?
3) What does the GDPR really mean for companies and for natural persons?

I shall conduct my empirical study by interviewing subject experts, who have experience of several GDPR projects at their customers. The interview will serve the research question number three. An interview on expert organisation will give me good overlook on the company perspective as these experts have worked with several different companies.

I will also look into news stream, mainly in Finland, regarding GDPR and reflect the interview findings to news. News stream study will serve the research question number two. As the regulation was enforced only six months ago, there is not yet enough scientific research available to make conclusions, how the GDPR has impacted all organisations daily life in Finland or in Europe.

At the interview I expect to get answers regarding the GDPR as a phenomenon as well as the practicalities of it. Therefore, I decided to ask the experts following questions:

1) How long the GDPR projects have been and what kind of project organisation there has usually been?
2) Has the project been more process or information system oriented and which one has caused more work for companies?
3) Was it clear from the beginning what to do or was there any confusion? And what was the most difficult thing to do?
4) What, in your opinion, is the GDPR compliance maturity level in smaller companies in general?
5) How have the most talked subjects (e.g. right to access/ right to be forgotten/ right of rectification) been seen in companies' daily lives?
6) If I request a report about my personal data, how can I make sure, that I get all the stored information, and that my information is not stored in automatic decision-making systems?
7) Although the initiative to data privacy project came from EU, do companies see it as a good thing, that may benefit them in the future or was the GDPR project just to meet the minimum requirements of the Regulation?

The questions had a broader meaning for a purpose, because I wanted the interviewed experts to answer with more than few words and share their views more broadly. I made couple specifying questions based on their replies of my interviewees. I was in particular interested, how the companies decided to approach the project. I was curious to learn, if the companies saw the project in a same way, and what lessons they might have learned.

4 What Has Happened Since Enforcement Of GDPR

My research question number two is to study, what has really happened so far, and to see, if there has been any court decisions or case studies in EU about GDPR. There has been a lot of news, publications, infographics, trainings, and other activities concerning the regulations since May 2018. I take a look into the activities to understand better, what measures the companies have taken and in what magnitude.

4.1 Economic Impact of GDPR To Companies

GDPR has been significant effort for companies inside and outside EU (who do business in EU). International Association of Privacy Professionals (IAPP) and consulting company Ernst & Young (EY), estimated that top companies in United States and United Kingdom have spent significant amount of money to comply with GDPR as illustrated below in Figure 2.

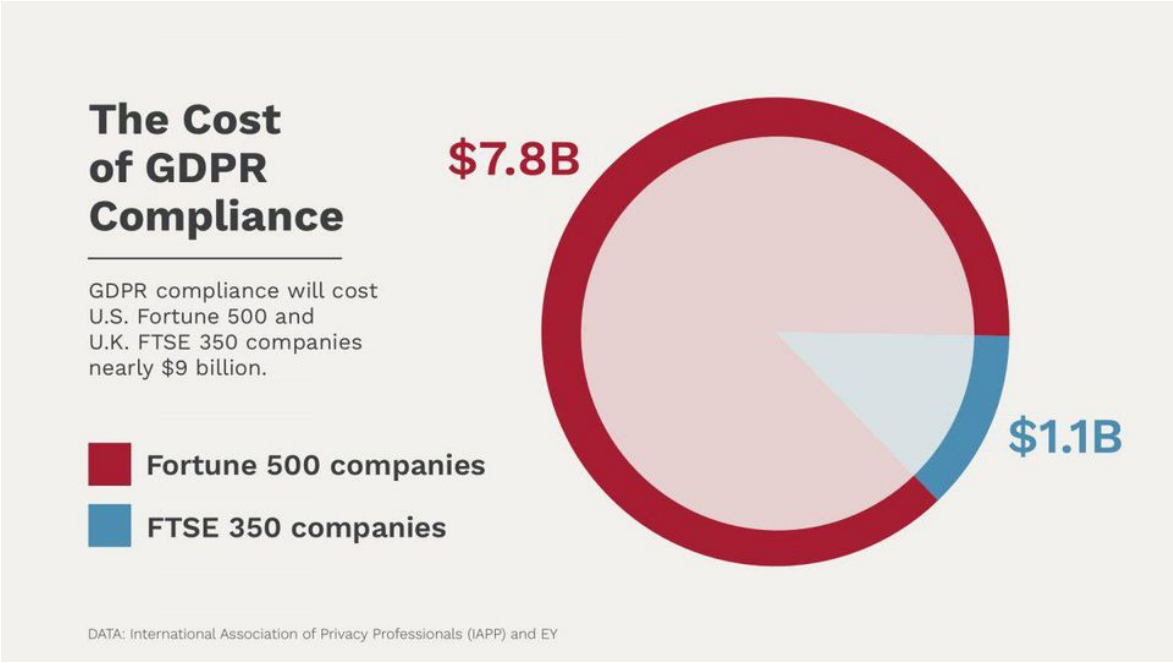

Figure2: The cost of GDPR Compliance

The study was conducted in 2017, well before the enforcement of GDPR. The companies expected costs to roll and not end by May 2018, since they were looking to hire employees to make sure they keep GDPR compliant.

Although the expense of GDPR per each company may be disputable, it is apparent that the shift to data protection in each organisation in EU area created a large business po-

tential. This potential attracted several companies to compete for their share of the market. The Finnish Data Protection Ombudsman, Reijo Aarnio complained that some consulting companies and education providers have misled their customers regarding the penalties, thus causing overreactions in their clientele (Pulkkinen, 2018).

SIA Partners studied economic impact on FTSE100 enterprises regarding the cost of compliance per industry and number of employees per company. Figures 3 shows the difference between different size enterprises (minimum 1000 employees) of costs accumulated from GDPR implementation. We can also notice how the average cost follows almost linear line until 10000 – 50000 employee's enterprises but gets much higher for bigger enterprises than that.

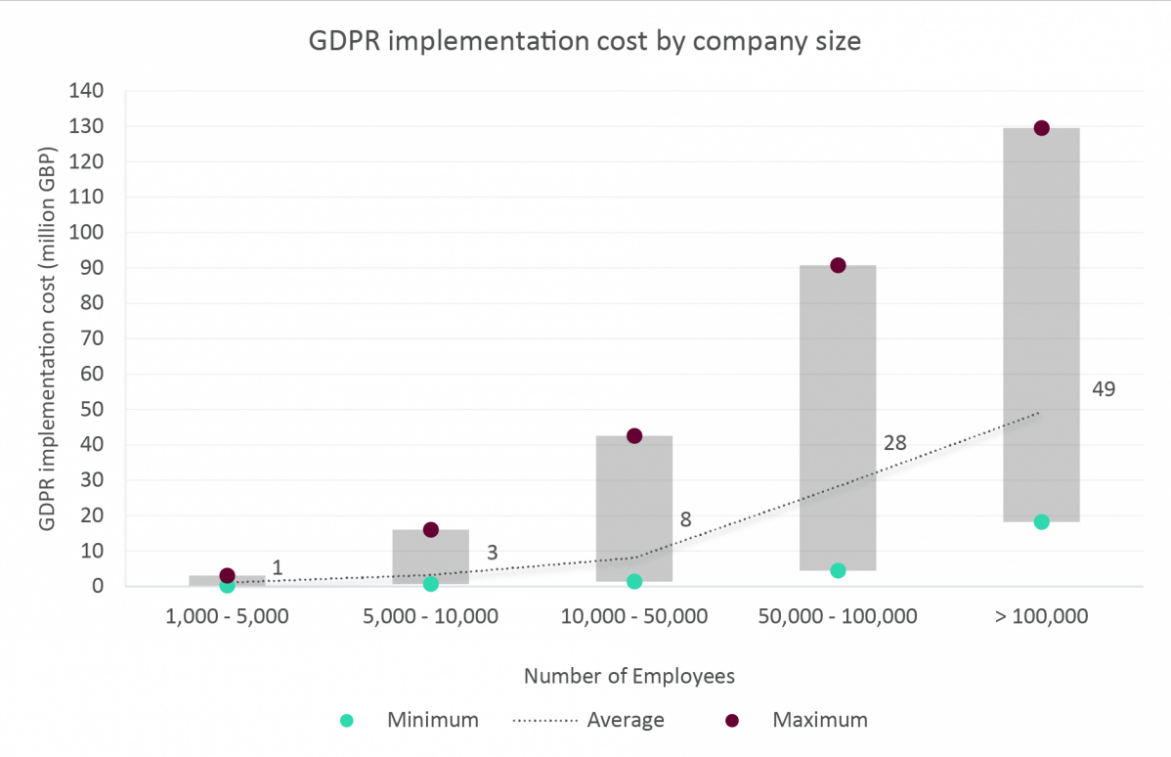

Figure 3: GDPR implementation cost by company size

Tobias Bräutigam, reluctantly, estimated a price tag for GDPR project to be anywhere between 100 and few million Euros (Bräutigam, 2016). He continued that the price depends on four factors: Industry and processed data, size of the company, maturity of data privacy protection in place, and investments to new IT-systems.

When talking about the cost of GDPR, it is easy to confuse the cost of implementation project and running costs per year to stay compliant. Both costs will take place and they don't necessarily correlate with each other i.e. higher cost of project does not mean lower cost of maintenance.

Figure 4 illustrates the costs for GDPR implementation by business sector. According to the graph, banking faces by far the biggest costs, trailed by energy, commodities & utilities, and retail goods. Aforementioned industries have large number of consumer clients and they process typically a large amount of private data, which explain the high cost of implementation project. The lowest expenses in Figure 4 are facing Media, Travel & Leisure, and Industrial Goods & Services. Surprisingly Health Care sector does not have high costs, regardless the nature of data they process and the number of private customers they have. One explanation may be the maturity of previous data protection work on this sector.

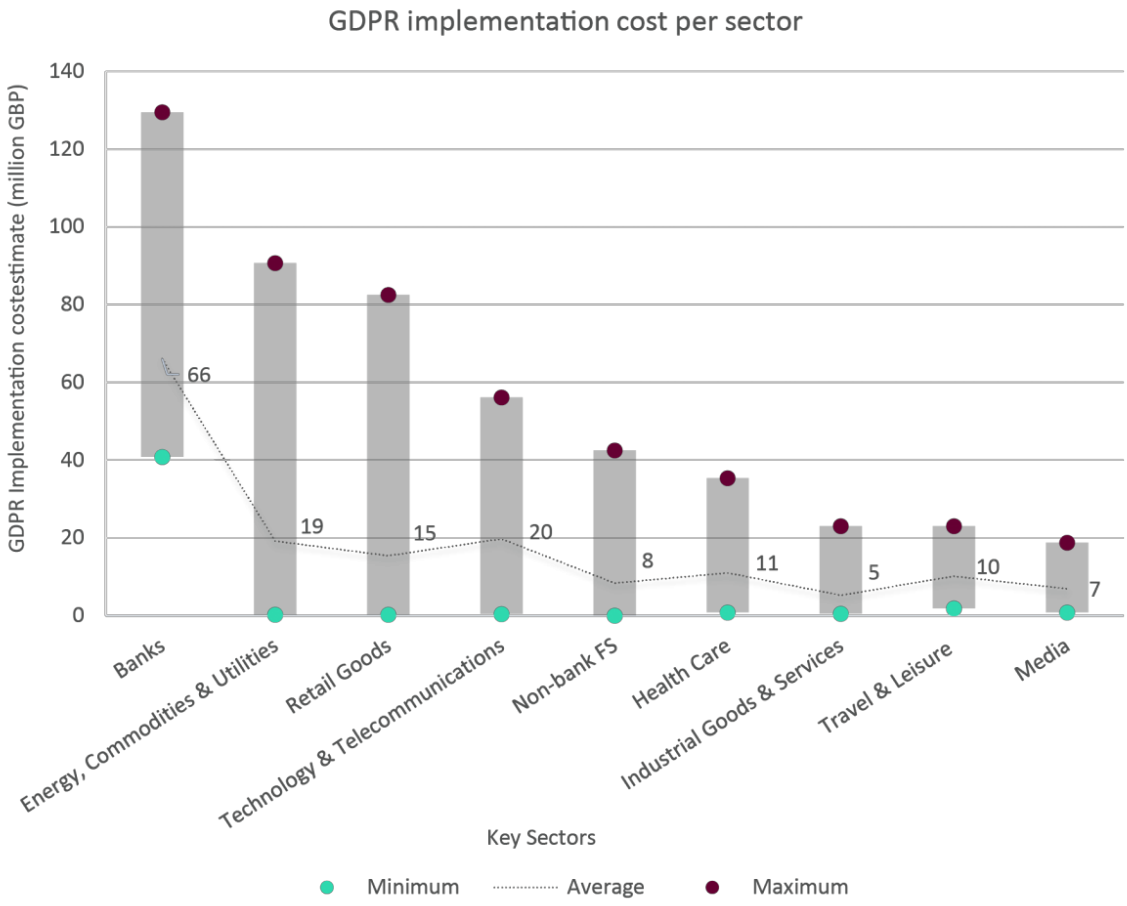

Figure 4: GDPR implementation cost by sector

SIA Partners estimated the average cost of GDPR compliance to be ca. 500€ per employee. Harri Leinonen from Pricewaterhouse Coopers (PwC) found 500€ per employee to

be too high figure and estimated 100 000€ being sufficient budget even for large companies (Pulkkinen, 2018). The difference in figures is interesting since for large companies the GDPR compliance project is estimated to take 12 to 18 months and employ tens of people, including external workforce. 100 000€ seems rather low figure but is naturally possible when the parameters mentioned by Bräutigam are favourable.

4.2 Court Cases Concerning Data Privacy

As GDPR was a hot topic in media for at least last six months before the enforcement date, I was curious to study, what has really happened ever since. While knowing that couple of months is too short time to evaluate the effects of the GDPR, I wanted to look into the first wave court cases regarding the GDPR.

In July 2018, two months after the enforcement of GDPR, the first court decision came from Germany. The decision was made in Bonn, Germany where American non-profit organisation was trying to collect more information through their partner about natural persons than necessary (Millar and Marshall, 2018).

Sweden has numerous GDPR-related court cases in process. Dagens Industri wrote on 25th September that there are 66 organisations under investigation related to violations of GDPR (Dagens Industri, 2018)

The Dutch Data Protection Authority initiated an GDPR investigation in late June 2018 to 30 randomly selected large companies in 10 different sectors in Netherlands. The investigation was to be performed “ex officio” (IAPP, 2018)

Finnish Data Protection Ombudsman Reijo Aarnio told in September 2018 that they have received more complaints than they expected. Since 25th May, his office has lodged ca. 800 complaints in 4 months when they expected 1500 complaints per year. On average, the number of lodged complaints has been 6 - 8 per day (Lännen Media, 2018).

In United Kingdom the respective figures for complaints are 500 phone calls to Information Commissioner’s Office per week. However, one third of those complaints fail to meet the criteria of data incident. Number of complaints has, as well as in Finland, increased dramatically: in 2017 number of complaints was 2417 between 25 May and 3 June whereas in 2018 the number was 6281 in same period (ITPRO, 2018).

High numbers of lodged complaints, early court decisions and ongoing legal processes suggest that data subjects have exercised their new rights to check what information is controlled and processed about them.

The Europol published an IOTCA report on September 2018 where researchers warned that GDPR sanctions have opened a new opportunity for criminals to extort their victims by their data loss (Europol, 2018). The risk of facing high sanction fees may lead companies to pay hackers a ransom rather than informing the National Data Protection Authority. The researchers continue that paying a ransom only funds criminal organisations and there is no guarantee that criminals would not disclose the data breach.

5 Empirical Results – interview and testing in real life

As the target of my thesis is to find out the real-life implications of GDPR and to find out companies' opinions on the new regulation.

Talentbase is a Finnish consulting company based in Espoo, Finland. Talentbase employs currently over 60 experts in digital services, including Privacy, Architecture design, Content Management, Service design and user experience, Advanced data analytics and AI, CRM, Data management and quality, and Lean services. I had a privilege to interview two of their data privacy experts about my research questions. The interview took place on 26th of September 2018 at Talentbase Headquarters in Espoo.

One of the most talked subjects in media during the GDPR transition period was natural person's requests of information to organisations. I wanted to understand, how different companies working in different fields of business implemented their GDPR projects. I also wanted to understand, what sort of project organisation was involved in, and what the road to GDPR compliance looked like for different organisations.

5.1 Data Privacy expert Interview Results

Question: How long the GDPR projects have been and what kind of project organisation there has usually been?

Answer: "All customers, Talentbase has helped regarding GDPR, are their existing customers. Talentbase was not the initiator of GDPR project, but on average the GDPR project has taken 1-1,5 years. In bigger companies there has been already some preliminary work done, but in more organised way the project has taken 1 – 1,5 years."

"We have 3 purely data privacy customers and more customers, where we have been consulting information management. In the latter we haven't strictly been consulting about data privacy, but we have raised awareness through "privacy by design" approach."

> **Sub question:** And all customer cases were in big companies, weren't they?
>
> **Answer:** "Yes, they were. All these three customer cases were in big companies. Project teams in our customer environments consisted of tens of consultants from different vendors."

Sub question: Do those tens of consultants include all system experts from e.g. ERP vendor?

Answer: “Yes, if it was needed to look into information systems. However, in general the participants were part of the data privacy program and different inhouse solution experts, who knew, where the privacy data in the systems is stored. The analysis of GDPR readiness was executed by external party.”

“When there was a need to look into data management and how the information flows within the house, the customer’s own IT crew participated. The variety of project personnel derived from different starting point in different customer cases. In big companies the GDPR project is not a 5-team member project. The project group needs to be big.”

“GDPR teams consisted of IT-system experts and lawyers. Lawyers helped to interpret the law in different occasions, but the project lead was on IT-experts. Also, communication was important because the message had to be clear, but at the same time comprehensive from legal point of view. The role of lawyers was therefore very important and in big companies GDPR project without legal advice would have been impossible.”

Question: Has the project been more process or information system oriented and which one has caused more work for companies?

Answer: “Big companies, which at the same time are not young companies anymore, have lot of legacy information systems that have been developed during history and documentation has been neglected partially or completely. It may simply be impossible to find documentation that would meet the GDPR requirements of accountability. It may also be hard to investigate, what information is stored in those systems, and how it flows between the systems, and who gets an access to this information.”
“There was so much work around the information systems that it has taken all the focus away from business processes. In retrospective, it might have been better to analyse the processes first and what information is processed in them. After the process analysis the next step would have been to see, what information systems support the business processes. This would have been more correct order of events, but apparently it has been easier to sell the idea of information system approach. Due to this, most of time and resources have been spent on analysing and working with information systems.”

“Although the sequence of the events could have been different, we and our customers have learned a lot during the GDPR project and most of all, the job has been done. I hope that companies have adapted the privacy in their everyday work, although there are signs of GDPR hangover, but when business processes change the companies would identify automatically the use of personal data in business processes.”

“It would be logical to approach the subject through the IT-systems, because they contain a lot of personal data, and data are as important as the processes are. However, the processes should be fixed first.”

“Our policy and philosophy are to be holistic, meaning that all things are related with each other. Rather than doing privacy, data governance, data management as a project, they should be part of our everyday job. A good example is IT-systems development, where the privacy and information security should be included automatically, when developing new services. Not only because of accountability, but also because the data can then be utilised better.”

“We would like to see the “privacy proofing” in all business functions e.g. customer service or development. Not all the workers need to be privacy experts and the support in data privacy and data protection should always come from the experts, but companies should adapt “privacy proofing” in their organisation culture.”

“The GDPR hangover is a symptom that not all the companies have data privacy in their culture yet and creating a culture takes time, but that should be the direction. Companies should consider how the data that they control affect the data subject’s life.”

Question: Was it clear from the beginning what to do or was there any confusion? And what was the most difficult thing to do?

Answer: “Luckily our customers’ GDPR projects were not totally outsourced and each customer had a team that had started the work already either from legal or practical side. Therefore, certain basic principles of data privacy had already been understood.”

“It was difficult to determine sufficient level of documentation related to accountability as the regulation did not directly dictate that. An education of basic concepts, like “what is personal data”, caused a lot of work to all employees. Regular employee may think that

personal data is only personal ID and therefore sees no need to analyse their processes. This shows, that the employee fails to understand the concept of data privacy."

"An expert may also have a one-sided point of view since for expert it is clear that IP address is personal information, but not necessarily to regular employees. So, a lot of work has also been done to make sure everyone talks about the same thing, when talking about data privacy. Another big issue was that the focus had been directed to IT-systems mainly, as a result the bigger picture suffered. Consequently, companies understood the importance of the bigger picture too late and systematic project approach was well forgotten. Companies tried to do everything at once and got nothing finished."

"Another challenge was companies' internal and external communication concerning GDPR. According to our observation, on 25th of May no companies entirely complied with GDPR. The main focus was on the parts that were visible outside the companies. Overreactions have occurred concerning data privacy like consent renewals, which were unnecessary sometimes. As an example, some companies sent a consent renewal letter despite the fact that customer's consent had been legitimate even before GDPR enforcement. From communicative point of view, it's nice to know, that company is aware of GDPR, but when most of companies flooded people's mailboxes right before the GDPR deadline, most of the messages went past unnoticed."

"Neither we, nor our customers needed to contact the data protection officials, but there were challenging topics like automated decision making and some other specific issues, that required some clarifications. It would have been useful to have better examples, how to determine, if a company is a data controller or processor, and to justify marketing without data subject's consent. This caused a lot of work, but the solution was a thorough documentation of the issue and proper explanation, why company decided to act in a certain way. Should there be a need to review the past actions, it is easier to look into previous documentation and adjust the further actions rather than have no previous work done at all."

"All in all, there's been a lot of confusion, but nevertheless it helped to improve the understanding. A lot of cooperation has been done between lawyers rather than with data protection ombudsman's office."

"Our mission is to tell about data privacy in common language. Typically, lawyers may be brilliant, but use legal jargon. Those people, who should understand and follow the privacy regulation in their work, don't understand, what the legal terms mean. This mismatch in

communication may cause misunderstandings or even message rejection. Change in company culture is based on message that people understand. In two of our bigger customer cases we worked with employees to show them, what privacy proofing meant in their everyday work."

"A challenge is to show, that GDPR doesn't only concern those functions of business that work directly with customers, but also if you print a spread sheet and leave it on a table. In the evening a cleaning lady may also see the same spread sheet on desktop and find someone's private information on it. There are in general so many single points of failure, that proper education and guidance is very much needed. All those process manuals should also be reviewed and there are so many details that most likely not all of the GDPR work could be finished by 25th of May 2018."

Question: What, in your opinion, is the GDPR compliance maturity level in smaller companies in general?

Answer: "It depends a lot on the field of business, and how regulated the business is. There are some business areas, like real estate dealers, who are more aware of privacy, thanks to their trade union's education. In cases where companies participate in their trade unions education, even smaller companies can have a good grasp on data privacy. Then again, there are some small companies, who work, for example, in infrastructure building, where GDPR has raised concerns, how to cope with data privacy in the future."

"The smaller the company is the less there are employees, who could focus full time on data privacy. There are big misunderstandings in even basic data privacy concepts and a fear of fines has caused an anxiety that "what should I do with the GDPR". As an example, one hair dresser was nervous about, what she should do regarding the GDPR. A question raises, how smaller companies should find time and resources to determine, what they should do to comply with GDPR, because reading the regulation won't give all the answers? We truly hope that there has been some affordable education available by trade unions or other parties who have managed to raise the awareness of their clients. "We should imagine that real estate dealers, who work more with laws and regulations, the GDPR hasn't been that big issue. But for hairdressers, who normally don't need to think about regulations that much and still communicate with their customers by email, the GDPR might have been nerve breaking."

“If the big companies, who have dedicated personnel for privacy, are relieved that the GDPR project is finally done and even in those it’s not entirely finished yet, how could the small companies be GDPR compliant?”

Question: How have the most talked subjects (e.g. right to access/ right to be forgotten/ right of rectification) been seen in companies’ daily lives?

Answer: “No, not really. There have been some report inquiries before GDPR and since May 25th the amount hasn’t increased. There were thoughts in bigger companies, who store personal data in several different IT-systems, that GDPR might bring a flood of inquiries. It turned out that such flood never came and that was a relief.”

“Some companies got prepared to reply information requests by attempting to automatize the data search as expected number of requests was big and manual searches would jam the organisation. This didn’t fortunately happen, and manual labour-based process is adequate. Manual process naturally is prone to human errors, but on the other hand, it is safer to check, what information is gathered and sent to the customer to avoid sending too much or wrong information.”

“We have been wondering, how smaller companies, who don’t have identity verification methods (e.g. TUPAS bank ID, mobile ID), can be sure about requestor’s identity?”

“We are under impression, that natural persons may be more active concerning data privacy and they may ask to see their personal data, but it hasn’t gone further than that e.g. erasure.”

“About erasure, based on experience there’s a lot of information that is gathered and processed in compliant way e.g. about existing customers. Then there are open questions like what information company can keep when about their non-active customers? The answer seems to be: “well, it depends…”

“How can company start to remove information from IT-system backups? No one seems to have an answer to that. If a company needs to restore their IT-system from backup and the backup brings back personal data of someone, whose data has already been erased, how can there be adequate answer to that?”

Question: If I request a report about my personal data, how can I make sure that I get all the stored information and that my information is not stored in automatic decision-making systems?

Answer: “We have been wondering about this too. If everything in the GDPR project the documentation of processes is done properly and it can be determined, where the information is stored and processed, then a company should know that. The question is - do they do the documentation properly?”

“As automatic decision-making is one of the major topics in GDPR, we would assume that all bigger companies had to take algorithms and automatic decision-making tools into consideration. “

“Giving an advice how to be sure that someone’s personal data is not used in automatic decision-making is difficult. A person may have a clue, e.g. how certain webstores work and then ask the company, if they use his/her data in automatic decision-making or targeting algorithm.”

“For sure, companies ask a requestor to specify, what information is requested. If we would get such a request, we would need to ask the requestor, if he/she is an old employee, customer, job applicant, etc. Practically all bigger companies, at least, need to filter the requests as they need to look into several different registers depending on requestors’ role.”

Question: Although the initiative to data privacy project came from EU, do companies see it as a good thing that may benefit them in the future or was the GDPR project just to meet the minimum requirements of the regulation?

Answer: “In general, companies have seen GDPR as a source of agony rather than source of joy, but mostly they have been annoyed with the schedule of compliance work that has taken the resources from other development projects of their business. But those employees, who have stayed in the company, and who work with privacy matter in their everyday work, have raised the general awareness of privacy within the company. Now that the seed of privacy thinking has been planted, and it would be important to embrace it and not to forget about it. Otherwise the great effort (GDPR project) goes down the drain. We witnessed, that the hard work resulted into deep knowledge within the company and employees recognised privacy matters in an exemplary way. It is great to notice that, and

it gives warm feeling, that business work according to legislation and customers' information is safe – that's important at the end of the day."

"In general trust is important in business, but very few, if any, have harnessed data privacy matters as their competitive edge. A lot of companies have thought of self-service portals, where natural persons can see, what their personal data is controlled. That has raised trust through transparency and may be partial reason of, why there hasn't been a flood of information requests. For most of us this may be enough, and no further questions arise in relation to e.g. automatic decision-making. "

5.2 Data Privacy expert Interview Analysis

Question: How long the GDPR projects have been and what kind of project organisation there has usually been?

Analysis: My goal was to find out, what kind of resources were needed and for how long the project should run. The answer was from 12 to 18 months in big companies. The demand for project team size was big as well "tens of consultants". This implies that GDPR was indeed seriously time and effort consuming project for bigger companies. I would imagine the demand of project team size will drop as the size of the company decreases. However, since GDPR is all about securing private data, the culture of the company needs to adapt, thus everyone in the organisation has to be involved. The amount of people involved in the process inevitably has relation with the economic impact to companies as discussed in chapter 4.1.

The interviewees' answers were in line with the different companies answers in media. The projects in big companies have taken, at least, a year or longer depending on the maturity level of data privacy prior to the GDPR. As sectors differ from each other by the amount of personal data required, the level of maturity varies as well, hence 12 to 18 months might be the most exact project duration estimate that is reasonable to give in big companies. In small companies the GDPR project has taken a lot shorter time to prepare their registers to comply with the Regulation. As an example, a small primary producer spent 4 hours for their project, while small recruiting company spent one month (Kempas, 2018).

Question: Has the project been more process or information system oriented and which one has caused more work for companies?

Analysis: According to the interviewees the main focus has been on information systems. Big companies tend to have a lot of information systems, new and legacy, that contain a lot of information and sometimes the documentation of the systems is poorly arranged. From this point of view the companies' focus on information systems is understandable and equally important as the focus on their business processes. The interviewees commented, that unfortunately the emphasised focus on information systems has taken focus from the business processes and approaching the business processes first and only then the information systems would have served the purpose better. According to SAS Institute global survey, 45% of companies had structured process in place for GDPR project (SAS, 2017). The interviewees notions of hassle in the companies seems then to be reality for most companies.

The main focus on information systems is understandable as they may be easier to document and possibly change than business processes. This explains as well, why system approach may be easier to accept for companies rather than analysing both business processes and information systems.

Most importantly the data privacy work has been done. However, as the interviewees say that companies are undergoing a GDPR hangover, have the companies had resources to investigate their business processes from data privacy point of view? Process approach would have possibly supported the data minimisation principle as companies would need to take a look into their processes and view, what information they need to function and what is unnecessary.

Question: Was it clear from the beginning what to do or was there any confusion? And what was the most difficult thing to do?

Analysis: The interviewees mentioned three general observations: lack of data privacy understanding, focusing only on information systems, and hassle in the GDPR project.

Data privacy education to all employees is an enormous task especially in big companies. Talentbase experts explained, that they went to regular employees' level to explain, what data privacy meant in their everyday work. This approach is time consuming, but efficient at the same time. A risk of making unwanted mistakes reduces, once everyone understands, what private data mean and what they should do with these data.

According to SAS Institute survey, the interviewed companies mentioned three biggest challenges in their GDPR preparations: How to know if we the actions we take to comply are sufficient, how to find stored data, and how to manage data portability and the right to be forgotten (SAS, 2017)?

Focus on information systems and hassle in the GDPR project seem to be partially related with each other, to my mind. As the interviewees revised the GDPR project in previous question, it would have been better to look into the processes first and then the information systems.

Hassle may be originated from different issues. According to the interview, the hassle began, when companies understood, how big the big picture of data privacy was versus how little time they had budgeted. I assume this was the first data privacy exercise for many companies in this magnitude, therefore it is understandable, that the size of the project overwhelmed companies.

Question: What, in your opinion, is the GDPR compliance maturity level in smaller companies in general?

Analysis: The interviewees had trust in those companies, who are more familiar with processing private data, but the concern was on those, who traditionally were not concerned about private data. The company size doesn't necessarily reflect their process complexity. The interviewees hoped, that trade unions or other parties had been active regarding educating their members. Naturally not all companies are members of their respective trade unions.

According to Federation of Finnish Enterprises, they have 115 000 members out of ca. 357 000 companies all together (Tilastokeskus, 2018). Even if most of the companies that are not members of Federation of Finnish Enterprises would be members of some other union, there would still be thousands of companies without trade union membership. From this point of view, the interviewees' concern about the GDPR education to all companies is understandable.

Most Finnish companies are small by the size of employees. In fact, 97,4% of Finnish companies have less than 20 employees (Tilastokeskus, 2018). Talentbase interviewees stated that not all companies, especially the small ones, could have a dedicated employee to take care of the company's GDPR compliance. This leaves a chance, that not all companies were GDPR compliant on 25th of May 2018 and may still not be.

Question: How have the most talked subjects (e.g. right to access/ right to be forgotten/ right of rectification) been seen in companies' everyday lives?

Analysis: The interviewees stated that the feared flood of information requests did not come, which was a relief. Petteri Järvinen shared this opinion on his blog as he wrote that the flood never came, and it was not a surprise (Järvinen, 2018).

Although the National Data Protection Ombudsman's office reported about increased contacts, the consensus seems to be, that natural persons are not more interested in the registers, they are mentioned in, than they were before the enforcement of GDPR. As Järvinen rightfully says, that we are only 6 months in and things can change.

As some bigger companies attempted to automatize the data collect per customer request, the interviewees estimated a manual process being adequate in most cases and safer too. Automatized query to registers and report without a control may compromise some information, that is not requested. I would assume, that it is a matter of time, when someone gets too much information by their information request.

The interviewees also mentioned, that while there may have been more information requests, there has not been further proceedings from there e.g. data erasure requests. There are several open-end scenarios about data erasure, that would need to be solved so perhaps the lack of requests works in favour of companies. The interviewees mentioned system backups and data about non-active customers as problematic subjects.

Question: If I request a report about my personal data, how can I make sure that I get all the stored information and that my information is not stored in automatic decision-making systems?

Analysis: The interviewees had been considering this issue as well and the only way to be sure is trusting the company's mechanism and documentation of controlled data. Naturally, there are extreme measures like full data audit to be sure, but natural persons do not get access to such tools.

Perhaps unsurprisingly this question is tough to answer and for a natural person total transparency of companies' mechanisms may be a distant dream. A person can get hints of being part of automated decision-making tools or algorithms, but not necessarily ever

be sure. In the future this may not be any easier as artificial intelligence solutions get more foothold in companies' business processes.

Question: Although the initiative to data privacy project came from EU, do companies see it as a good thing that may benefit them in the future or was the GDPR project just to meet the minimum requirements of the regulation?

Analysis: PricewaterhouseCoopers conducted a pulse survey on companies in United States about GDPR prior to its enforcement. The survey concluded that some companies intended to make the GDPR compliance a market differentiator to those who are non-compliant (PwC, 2018). SAS Institute mentioned in their survey the top 3 benefits of becoming GDPR compliant: Data governance will improve, General IT capabilities will improve, and image will improve (SAS, 2017).

I was curious to find out, if my interviewees had noticed similar development in companies they had worked with. Their answers were rather the opposite and on a contrary the GDPR was more agonising project, than competitive edge creator. For not knowing their sector these companies work in, it is not possible to say, whether this is well or ill advised. However, the trust of companies conducting their business with respect towards their customers is ever more important, and perhaps even these companies should consider data privacy as a market differentiator.

Most importantly the interviewees saw the general understanding of the data privacy thinking improved at their customers and that it should be embraced and not let all the hard work go down the drain in the future. Most likely the upcoming initiatives on national and EU regulations regarding data privacy will keep the data privacy on top of agenda of each company in European Union.

5.3 Self-probing Cumulative Results

Article 15 of GDPR grants a right for an individual to request a report from every organisation of collected information. As mentioned in chapter one, there are several different operations an individual may proceed with according to the report e.g. consent withdrawal, request for correction, request to be forgotten. A natural person's point of view on GDPR is important since the core of the GDPR is to protect natural person's data.

I performed a study to three different organisations to probe, what my personal data are controlled. One company is a transportation company and two companies work on a consumer retail market. All selected companies provided the report within 30 days of the request; some provided it right away or next day and some provided it couple of days before the deadline.

I received from each company a lengthy cumulative report or a set of reports from different registers. The controlled information categories about me are given in the table below.

	Customer retail company A	**Customer retail company B**	**Transportation company**
Full name	yes	yes	yes
Address	yes	yes	yes
Previous address	yes	yes	no
Phone number	yes	yes	yes
email	yes	yes	yes
Social security ID	yes	no	no
Date of birth	yes	yes	yes
Sex	yes	yes	yes
Bank account number	yes	no	no
Passport copy	no	no	yes
Marketing permissions	yes	no	yes
Profession	no	no	yes
Membership date	yes	yes	yes
Membership channel	yes	no	yes
Family role	yes	yes	no
Bonus dates	yes	yes	yes
Bonus amounts	yes	yes	yes
Purchase amounts per money	yes	yes	yes
Purchase amount per visit	yes	yes	yes
Partnership deals	yes	no	no
Bonus card details	yes	yes	yes

Electronic services details	yes	yes	yes
Customer groups	yes	yes	yes
Service requests and orders	yes	yes	yes
Service denials	yes	yes	yes
Employee information	yes	no	no
Detailed purchase information	yes	yes	yes

Table 1: Self-probing cumulative results

5.4 Self-probing cumulative Analysis

When comparing the results of the companies it is expectable to get different answers in different data categories. While both customer retail companies have similar core business, both have different additional service lines and for that reason the information they control, and process is different.

We can see that the data categories controlled by the companies are surprisingly similar and deviations are explainable. For example, customer retail companies do not need a copy of a passport and a company that pays customer loyalty points to bank account in money needs customer's bank account details. Consumer retail company B seems to collect less information from their customers, than consumer retail company A.

Looking back to chapter 2.5, the data report should have the following dimensions:

a) processing purposes,
b) categories of data,
c) recipients or category of recipients,
d) planned duration of storage,
e) information about data subject's rights (erasure, rectification, restrictions),
f) instructions how to file a complaint to authorities,
g) information about data origin,
h) existence of any algorithm-based processing of the data and consequences of such procedures,
i) possible distribution of personal data to external parties or countries without appropriate level of data protection.

Reflecting the received reports, none of the probed companies explained dimension a, d, g, h, and i. So, information was missing in 5 dimensions out of 9. Most of all I am interested in duration of storage and purpose of controlling my previous address or shopping habit information.

All in all, both customer retail companies built a customer-oriented interfaces to order the report about someone's personal data. The bigger the companies get, the more registers they usually either control or process. As Talentbase experts said at their interview, companies were afraid of the flood of data requests and they would need to filter the requests in order to serve the customer better and on the other hand not to jam their internal processes due large number of information searches. Perhaps for this reason both customer retail companies designed a user interface, where a person can select the category of register, he/she would like to get a report from e.g. employee register, customer register, etc.

Unlike the consumer retail stores, the transportation company had not created a portal, but a webform for individuals to fill and print and in the end to send them by secure email. The request was to be accompanied by a copy one's passport. Although this method inevitably fulfils the requirement for right of access, it is cumbersome and not as customer service oriented as of those consumer retail companies.

I wanted to request a report from a large logistics company, but when they instructed to send the request by a letter to abroad, I decided not to pay an effort.

6 Conclusion

To conclude the thesis, the best way is to look back in reflection of my research questions. The most interesting concepts of GDPR are relatively same for natural persons and companies. The increased transparency of person's private data increases individual's trust to companies, but simultaneously causes extra trouble to companies, who are obliged to look critically into their business processes, and information systems and to look into the ways to prove their accountability.

Germany was the first country to give a court decision to a company for collecting too much information from their customers, thus violating the data minimisation principle (see chapter 4.2). Several other data protection investigations are underway, and the near future will tell us, what their verdicts are.

Companies have mainly seen the GDPR as a nuisance rather than value adding project (see chapter 5.1). The project has taken on average 12 to 18 months and involved tens of people. The cost of GDPR compliance varies and exact number is hard to determine. Estimations are 500 dollars per employee to 100 000 euros even in big companies (see chapter 4.1). Since the magnitude of the project, many companies had to postpone their other development projects, and this naturally raised criticism. It was important to educate all employees to understand, what private data meant, and how they should take it into consideration in their everyday work.

To get a better view on companies' sentiment I decided to interview a consulting company, which worked daily with different customers. The interviewees' answers followed closely the information on media and no contradictions in major subjects, except on benefits of the GDPR occurred.

The General Data Protection Regulation is an interesting subject to study. I began my thesis couple of weeks after the enforcement date. Currently, the enforcement date was 6 months ago and since then a lot of news has been circulated in mass media about the GDPR. According to some news nothing much has happened, but contacts to Data Protection Ombudsman's office regarding complaints has increased greatly. Same phenomenon is visible in also elsewhere in Europe.

Regarding the GDPR, I believe that a lot is still to come. National data protection law has just passed, and the Data Protection Ombudsman has obtained its jurisdiction, and now we shall see, how the regulation and its penalties will be applied.

The experts say, that all companies have still work to do to comply with the Regulation. I have collected a checklist in Appendix 9, in Finnish, what small companies should ensure to meet, when assessing how solid ground they are standing on regarding the GDPR.

The relationship of AI and GDPR is yet to be defined - algorithms need data to get better, but GDPR constrains the free use of private data. We are going to see, which one of them will prevail or whether they can compromise.

The interviewees of my research said that even though the companies have seen the GDPR project as time consuming and agonising, the seed of data privacy thinking is planted. Although the GDPR was a compliance project, the nature of data protection is a process and all companies must stay accountable for their actions in the future too.

It would be interesting to further investigate the companies, which would critically review the data they collect to provide their service in good faith.

References

Afifi-Sabet K, 2018. IT PRO. Companies “over-reporting” data breaches as ICO takes 500 calls per week. URL: https://www.itpro.co.uk/information-commissioner/31912/companies-over-reporting-data-breaches-as-ico-takes-500-calls-per. Accessed: 3rd November 2018.

Björkman F, 2018. Dagens Industri. Om två veckor faller domen: Här är bolagen som hotas av GDPR-böter URL: https://digital.di.se/artikel/om-tva-veckor-faller-domen-har-ar-bolagen-som-hotas-av-gdpr-boter Accessed 19th October 2018.

Bräutigam T, 2016. International Association of Privacy Professionals. How to budget for a GDPR project: A Primer. URL: https://iapp.org/news/a/how-to-budget-for-a-gdpr-project-a-primer/. Accessed 23rd September 2018

Cavoukian A, 2018. Privacy by Design, The 7 Foundational Principles. URL: https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf. Accessed 24th July 2018.

Eduskunta, 2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi URL: https://www.eduskunta.fi/FI/vaski/Kasittelytiedot-Valtiopaivaasia/Sivut/HE_9+2018.aspx. Accessed 14th November 2018.

Elinkeinoelämän keskusliitto, 2018. Tietopaketti yrityksille: EU:n yleinen tietosuoja-asetus ja tietosuojalaki. URL: https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/#6--Tarkistuslista. Accessed: 19th November 2018

EUR-Lex, 2018. Protection of personal data 95/46/EC. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046. Accessed 26 May 2018.

Eur-Lex, 2018. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Accessed 26th May 2018.

Euroopan komissio, 2018. Tietosuoja, paremmat säännöt pienten yritysten kannalta. URL: https://ec.europa.eu/finland/sites/finland/files/eujus15a-1631-i01_-_data_protection_infographic_-_infographie_fi-v03_lr.pdf. Accessed: 19th November2018

European Data Protection Supervisor. Legislation. URL: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Accessed 24th July 2018

European Data Protection Supervisor. The History of General Data Protection Regulation. URL: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Accessed 28th May 2018

European Union, 2018. Regulations, Directives and other acts. URL: https://europa.eu/european-union/eu-law/legal-acts_en. Accessed 26 May 2018

Europol, Internet Organised Crime Threat Assessment 2018, page 28. URL: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. Accessed: 3rd November 2018.

Järvinen P, 2018. Tietoviikko. Gdpr + 6 kk: mitä on tapahtunut? URL: https://www.tivi.fi/blogit/gdpr-6-kk-mita-on-tapahtunut-6748303. Accessed: 10th November 2018.

Kempas, K, 2018. Helsingin Sanomat. Luomuviljelijä laati A4-paperiarkin laajuisen selosteen, ohjelmisto-yritys käytti selvitykseen kuukauden – näin tietosuoja-asetus vaikuttaa yrityksiin. URL: https://www.hs.fi/talous/art-2000005692252.html. Accessed 4th November 2018.

Millar S.A., Marshall T.P. 2018. German Court Issues First GDPR Ruling. URL: https://www.natlawreview.com/article/german-court-issues-first-gdpr-ruling. Accessed 23rd September 2018

Nuotio T, 2018. EU:n tietosuoja-asetuksen myötä on ilmoitettu jo noin 800 tietoturvaloukkausta – "Hirveä määrä", kommentoi Reijo Aarnio. URL: https://www.ts.fi/uutiset/maailma/4079308/EUn+tietosuojaasetuksen+myota+on+ilmoitettu+jo+noin+800+tietoturvaloukkausta++Hirvea+maara+kommentoi+Reijo+Aarnio. Accessed 19th October 2018.

Office of Data Protection Ombudsman, 2018. Demonstrate your compliance with data protection regulations. URL: https://tietosuoja.fi/en/accountability. Accessed: 10th November 2018.

Pulkkinen S, 2018. Helsingin Sanomat. Konsultit ratsastivat EU:n tietosuoja-asetuksen uhkakuvilla – Tietosuojavaltuutetun mukaan jättimäisillä viranomaissanktioilla uhkailu oli täysin väärin. URL: https://www.hs.fi/kotimaa/art-2000005730671.html. Accessed on 23rd September 2018.

PricewaterhouseCoopers, 2018. Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies. URL: https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html. Accessed: 4th November 2018.

SAS Institute, 2017. GDPR readiness: Are you prepared for the May 2018 deadline? URL: https://www.sas.com/content/dam/SAS/bp_nordic/doc/Infographic/gdpr-readiness-109060.pdf. Accessed 10th November 2018.

SAS Institute, 2018. Survey: Only 7 percent of businesses GDPR-compliant as deadline looms, data privacy gains prominence. URL: https://www.sas.com/en_us/news/press-releases/2018/april/gdpr-survey-data-management.html. Accessed 10th November 2018.

Sia Partners, 2018. Figure 3 & 4, Preparing for the GDPR – Why you need £15m or £300-£450 per employee on average to implement the GDPR. URL: http://en.finance.sia-partners.com/20180115/preparing-gdpr-why-you-need-ps15m-or-ps300-ps450-employee-average-implement-gdpr. Accessed 23rd September 2018

Smith, O, 2018. Figure 2 The GDPR Racket: Who's Making Money From This $9bn Business Shakedown. URL: https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#4fbdb02134a2. Accessed 23rd September 2018

Tilastokeskus. Suomi Lukuina 2018, page 49. URL: http://www.stat.fi/tup/julkaisut/tiedostot/julkaisuluettelo/yyti_sul_201800_2018_19691_net.pdf. Accessed 10th November 2018.

Terstegge J, 2018. International Association of Privacy Professionals. Dutch DPA lauches ‘ex officio’ GDPR-Compliance investigation. URL: https://iapp.org/news/a/dutch-dpa-launches-ex-officio-gdpr-compliance-investigation/. Accessed: 3rd November 2018.

Wilhelm, E.-O., 2016. Figure 1, A brief History of the General Data Protection Regulation. URL: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protectionregulation. Accessed 25th July 2018.

Appendices

Appendix 1. Disclosed GDPR Report Consumer Retail Company A part 1

Appendix 2. Disclosed GDPR Report Consumer Retail Company A part 2

Appendix 3. Disclosed GDPR Report Consumer Retail Company A part 3

Appendix 4. Disclosed GDPR Report Consumer Retail Company A part 4

Appendix 5. Disclosed GDPR Report Consumer Retail Company A part 5

Appendix 6. Disclosed GDPR Report Consumer Retail Company A part 6

Appendix 7. Disclosed GDPR Report Consumer Retail Company B

Appendix 8. Disclosed GDPR Report Transportation Company

Appendix 9. Miten Suomessa ohjeistetaan pieniä yrityksiä toimimaan?

Lukuisat eri tahot ovat julkaisseet omia oppaitaan yrityksille toukokuussa 2018 voimaan astuneen tietosuoja-asetukseen varautumiseksi ja osoitusvelvollisuuden ylläpitämiseksi. Yritykset koosta riippumatta ovat saman arvoisia asetuksen edessä – kaikkia koskevat samat säännöt, mutta kaikkien ei tarvitse menetellä samalla tavalla. Vaikka pienillä yrityksillä toimintaympäristö olisikin helpompi kuin isoilla yrityksillä, rajallisemmat resurssit saattavat aiheuttaa enemmän päänvaivaa.

Elinkeinoelämän keskusliitto on laatinut tarkistuslistan yrityksille asioista, jotka tulisi ainakin ottaa huomioon, jotta tietosuoja-asetuksen vaatimuksia noudatettaisiin (EK, 2018):

- noudatetaanko henkilötietojen käsittelyssä asetuksessa määritettyjä henkilötietojen käsittelyssä noudatettavia periaatteita
- onko henkilötietojen käsittelylle asetuksessa tai kansallisessa lainsäädännössä säädetty laillisen käsittelyn peruste
- onko tietojen käsittelyä koskeva dokumentointi (ml. seloste käsittelytoimista ja muu käsittelyä kuvaava dokumentointi sekä sisäinen ohjeistus) riittävän kattavaa ja ajan tasalla – tämä on tärkeää osoitusvelvollisuuden takia
- ovatko käsittelyn turvallisuutta ja tietojen suojaamista koskevat toimenpiteet riittävät ja onko yrityksellä prosessia mahdollisista tietoturvaloukkauksista ilmoittamista varten
- onko henkilötietojen käsittelyn ulkoistuksia koskevia sopimuksia ja muuta ulkoistuksia koskevaa dokumentaatiota tarpeen päivittää vastaamaan asetuksen vaatimuksia
- edellyttääkö asetus tietosuojavastaavan nimittämistä
- onko rekisteröidyille annettava informaatio riittävän kattavaa ja selkeää – tämä on tärkeää läpinäkyvyyden takia
- pystytäänkö rekisteröityjen oikeuksia koskevat vaatimukset täyttämään
- noudatetaanko mahdollisissa henkilötietojen siirroissa EU:n ulkopuolelle asetuksen sääntelyä

Euroopan komission julkaisemassa esityksessä ohjeistetaan yrityksiä kiinnittämään huomiota seuraaviin asioihin:

- Viestintä
    - käytä selkeää kieltä,
    - kerro kuka olet, kun pyydät tietoja,
    - kerro miksi käsittelet heidän tietojaan, kuinka kauan niitä säilytetään ja kenelle ne luovutetaan.

- Varoitukset
    - kerro ihmisille tietoturvaloukkauksista, jos heihin kohdistuu vakava uhka
- Suostumus
    - pyydä ihmisiltä selkeä suostumus tietojen käsittelyyn,
    - jos keräät tietoja lapsilta sosiaalista mediaa varten, tarkista ikäraja, joka määrittää, tarvitaanko vanhemman suostumus.
- Tarkastelu ja siirto
    - Anna ihmisille mahdollisuus tarkastella tietojaan ja siirtää ne toiselle yritykselle.
- Arkaluonteisten tietojen turvaaminen
    - Toteuta ylimääräisiä suojatoimia terveyttä, rotua, sukupuolista suuntautuneisuutta, uskontoa ja poliittisia näkemyksiä koskevien tietojen turvaamiseksi.
- Pyyhi tiedot
    - Anna ihmisille oikeus ”tulla unohdetuksi”. Pyyhi heidän henkilötietonsa, jos he sitä pyytävät, mutta vain, jos se ei rajoita ilmaisunvapautta tai mahdollisuutta tekemästä tutkimusta.
- Markkinointi
    - Anna ihmisille oikeus kieltäytyä suoramarkkinoinnista, johon käytetään heidän antamiaan tietoja.
- Profilointi
    - Jos käytät profilointia oikeudellisesti velvoittavien sopimusten (esim. lainat) hakemusten käsittelyyn, sinun on kerrottava siitä asiakkaillesi, varmistettava että prosessin tarkistaa ihminen eikä kone. Jos hakemukseen vastataan kielteisesti, on tarjottava hakijalle oikeus riitauttaa päätös.
- Tietojen siirto EU:n ulkopuolelle
    - Tee oikeudellisia järjestelyjä siirtäessäsi tietoja maihin, joita EU:n viranomaiset eivät ole hyväksyneet.

Euroopan komissio ohjeistaa pieniä- ja keskisuuria yrityksiä tarkastelemaan omaa rekisterinpitovelvoitettaan. Rekisteriä henkilötiedoista tulee ylläpitää, mikäli tietojen käsittely on säännöllistä, uhkaa ihmisten oikeuksia ja vapauksia, tai koskee arkaluonteisia tietoja tai rikosrekisteritietoja.