GDPR COMPLIANCE IN NORWEGIAN COMPANIES

Wanda Presthus, wanda.presthus@kristiania.no
Hanne Sørum, hanne.sorum@kristiania.no
Linda Renate Andersen, linda.andersen@protonmail.com

Westerdals Department of Technology, Kristiania University College,
Christian Krohgs gate 32, 0186 Oslo, Norway

Abstract
The General Data Protection Regulation (GDPR) became effective from May 25th, 2018 in the EU and influences any company that collects and stores personal data about European citizens. Our research aim is to explore opportunities and challenges that Norwegian companies face when complying with GDPR. First, we studied the 99 articles that constitutes GDPR. Second, we conducted a survey questionnaire and third, we took part in the GDPR project of one large company during spring 2018. Our contribution consists of insights and descriptions of opportunities and challenges that Norwegian companies face when complying with GDPR. Our main findings include that the majority of our respondents was well informed about the new regulation and they rated themselves as well prepared. They even saw some positive aspects, like gaining more control over the company's data and business procedures. The greatest concern is how to comply with Article 17: Right to erasure ("right to be forgotten"). In addition, this paper contributes by identifying eleven of 99 GDPR articles that primarily influence a company's IT-systems. Our study should be of interest to company managers and it will remain relevant in the time after the GDPR implementation date. In this regard, one of our respondents eloquently stated: "Complying with GDPR is not a goal to be reached, it is the start of a journey".

Keywords: GDPR, information privacy, compliance, organisational perspective, explorative study

1. INTRODUCTION

"*If people cannot trust that information about them is being handled properly, it may limit their willingness to share information – for example with their doctor, or on social media. If we find ourselves in a situation in which sections of the population refuse to share information because they feel that their personal integrity is being violated, we will be faced with major challenges to our freedom of speech and to people's trust in the authorities*" (The Norwegian Data Protection Authority, 2018[a]). These lines demonstrate that privacy and legal security are vital to everyday life and in 2018, higher on the agenda than ever before. By introducing the General Data Protection Regulation (GDPR), more than 40 laws in Europe will be replaced (European Parliament, 2016; Justis- og beredskapsdepartementet, 2017, p. 13). GDPR is by far the biggest change in privacy over the last 20 years and has been developed to protect personal data (Rightbrain, 2018). In addition, GDPR introduces stronger penalties: if a company fails to comply with the new regulation, fines can be up to 4% of the annual turnover or up to 20 000 000 Euro, whichever is the highest amount.

Consequently, GDPR is linked to basic rights every individual has in our digital community, in addition to personal data that are collected and stored physically. But what are personal data? According to GDPR's *Article 4: Definitions*, 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 […] that natural person".*

Please cite as: Presthus, W., Sørum, H. & Andersen, L.R.: GDPR Compliance in Norwegian Companies (2018). Paper presented at NOKOBIT 2018, Svalbard, 18-20 Sept. NOKOBIT, vol. 26, no. 1, Bibsys Open Journal Systems, ISSN 1894-7719.

Moreover, this new regulation is applicable to all companies that handle personal data in the EU, and any company outside of the EU doing business within the EU. According to a survey based on 611 participants presented at The Norwegian Computer Society (Den Norske Dataforeningen) in February 2017, less than half of the Norwegian companies were prepared for the new regulation (Bark, 2017). Most likely, many organizations still struggle with complying with GDPR, also after the implementation date of May 25th, 2018.

"Every organization needs to adjust their processes and routines, and many need to change or acquire new system solutions when GDPR enters into force" (www.cw.no) and *"After the introduction of GDPR, I will own my own data"* (http://arbeidsnytt.no). These citations presage changes that will influence use of personal data in the coming years, as well as how this new regulation puts a pressure on most organisations. Consequently, GDPR is a cross-disciplinary field with several stakeholders, including authorities, lawyers, managers, technologists, IT developers, consumers, and more (Colesky, Hoepman, & Hillen, 2016). In the present paper, we emphasise the organisational perspective. Unlike, for example, the decision of implementing an information system to handle a company's resources (known as ERP systems) or customers (known as CRM systems), complying with GDPR is not optional for any organisation that stores personal data.

Challenges can be linked to various factors, such as the interpretation of new regulations, the motivation for organizational changes, and the management of collecting and storing personal data. Facing the fact that we have a limited knowledge about how this new regulation will work in practice, the research aim of this paper is to explore important opportunities and challenges that Norwegian companies face when complying with GDPR, at the time of the implementation of this regulation.

The rest of this paper is organized as follows. Section 2 describes the background and the selected eleven articles of GDPR emphasized in this paper, while Section 3 deals with related work. In Section 4 we present our method, followed by findings and discussion in Section 5, along with suggestions for further research. Concluding remarks are given in Section 6.

2. SETTING THE SCENE: DESCRIBING SELECTED ARTICLES FROM GDPR

The General Data Protection Regulation (GDPR) will influence every company that collects and stores personal data related to EU citizens. GDPR is currently a hot topic in Norway and the media regularly publishes articles regarding this subject. Many consulting companies and lawyers offer information and various services related to GDPR. The consequences can be severe if you fail to comply with the regulation. Based on the 99 articles (as found on the official websites; www.eugdpr.org and https://gdpr-info.eu) we have chosen to focus on eleven articles in this study, after careful review of all. We argue that it is primarily these articles that influence the company's IT systems and the data management. Below follows a short presentation of the selected articles, and more description is found in the Appendix:

Article 5: Principles relating to processing of personal data
Your personal data shall be processed with fairness, lawfulness and transparency, and only collected for specified, legitimate and explicit purposes.
Article 7: Conditions for consent
You can withdraw the consent at any time, and in an easy manner.
Article 15: Rights of access by the data subject
You can obtain confirmation to whether or not personal data concerning you are being processed.
Article 17: Right to erasure ("right to be forgotten")
You have the right to have some of your personal data erased from the organisation.
Article 20: Right to data portability
You have the right to receive your personal data, and reuse it for your own purposes. It allows you to move, copy or transfer personal data easily from one IT environment to another in a secure way.
Article 22: Automated individual decision-making, including profiling

You have the right to not be subject to a decision based solely on automated processing (without any human involvement).

Article 25: Data protection by design and by default

The organisation must ensure that your personal data which are necessary for each specific purpose of the processing are processed.

Article 30: Records of processing activities

The organisation must maintain a record of processing activities under its responsibility, such as: the name and contact details of the controller, joint controller, and data protection officer.

Article 32: Security of processing

The organisation must identify the scope of the assessment and perform a risk assessment.

Article 33: Notification of a personal data breach to the supervisory authority

The organisation must report the breach to the supervisory authority within 72 hours.

Article 37: Designation of the Data Protection Officer

The organisation must designate a data protection officer if it is a public sector, or, if private sector and carrying large scale systematic monitoring of individuals.

In sum, we believe that these eleven articles in particular will strengthen the rights of the individual, which was indeed the EU's motivation. Moreover, they will influence data management and various information systems in organisations. For example, let us imagine that you as an individual consumer has decided to purchase a new sofa for your living room from "Furniture Ltd" (fictive name). Prior to GDPR, both browsing the Internet and visiting the physical store would usually result in "Furniture Ltd" collecting large amounts of data about you, without your knowledge. Technologies such as surveillance cameras, people counting systems, beacons, web beacons, cookies and MAC addresses would be harvesting your personal data behind the scenes – even before you had made any purchase (Presthus & Andersen, 2017).

Let us say that you now request a brochure thorough the company's website. *Article 5* will for example influence how a marketing department collect and handle data about customers. Only a minimum of data is to be collected, meaning that in order for "Furniture Ltd" to send you the brochure per physical mail, you should not have to give up for example your telephone number. *Article 7* is about informed consent, and means that you have the right to clear (and short!) text that constitutes "terms and conditions". Also, pop-up messages on webpages with "This website uses cookies to give you better service" will have to be replaced with more detailed choices and opt-out for you.

Pretend that you have purchased a sofa, but you keep getting advertisement both in your mailbox and your e-mail inbox. If you did indeed sign up for newsletters, you have the right to withdraw it as easily as you gave it. Moreover, *Articles 15* and *17* give you the right to access all of the data that "Furniture Ltd" has accumulated about you, and you may request insight *(Article 15)* or even to have large parts of your personal data deleted *(Article 17)*. We have to keep in mind that some laws and regulations will take precedence over GDPR; for example, if you chose to pay by credit card it will not be possible to delete this transaction.

The concept of data portability *(Article 20)* is perhaps better explained by using a telephone company as example. If you have been subscribing to "Telephone Company A" for years, but want to switch to the competitor, you have the right to obtain all data about you, in a readable format. Then you can present your accumulated data to "Telephone Company B" and start to bargain: "Look at the large amount of SMS that I have sent every day for the past ten years. Please give me a better deal." "Telephone Company A" has 30 days to comply according to GDPR, but may be extended to 60 days for particularly large or complex request.

We included *Article 22: Automated individual decision-making* because of the rapid advances of technology. For example, more and more decisions are being conducted without any human involvement (Davenport & Kirby, 2016). Typical examples are recommendation systems as used extensively by Amazon, and loan calculators used by banks. Several banks will have a function on the website, where you enter your age, salary and other personal data, and the calculator will automatically decide if you

qualify for a loan. This technology is rapidly advancing, and now includes medical advice (IBM's Watson), which are based on textual data. We suspect that we will soon experience students writing essays that will be read and assessed without any involvement from a lecturer. We dare to claim that such technologies are here stay and GDPR will not make them illegal, however, the individual has the right to be informed. Another study conducted towards individuals (Presthus & Sørum, 2018) asked specifically about the students' viewpoint on automated grading on written exams. (Multiple choice exams have to a large extent been automated for a long time.) The results were that they were sceptical, but not entirely negative. They commented that technology for example is less biased that lecturers, but that they would prefer some human quality assurance in addition. Another concept related to *Article 22* is *price discrimination* (Martin, 2015). If you as a consumer book a hotel room through a website, your IP-address will automatically be mapped and recognized as belonging to a "wealthy or not nation", which again will determine the final prize of the hotel room.

In our examples above, *Articles 25, 30* and *32* will be less transparent to the individual, but they do serve as foundation for the other articles that we have previously described. *Article 25*: *Data protection by design and by default* primarily influences the IT developers and software engineers in an organisation. The Norwegian Data Protection Authority offers a 7-step guide for developers. The seven guidelines are: Training, Requirements, Design, Coding, Testing, Release, and Maintenance. According to The Norwegian Data Protection Authority this article is closely related to *Article 22: Automated individual decision-making,* because the aim is to offer transparency (The Norwegian Data Protection Authority, n/d). *Articles 30* and *32* deal with assigning responsibility to roles in the company, so that the company will be prepared in case of data breach *(Article 33)*. If personal data should be stolen, unintentionally deleted, lost, or subject to unauthorised access, the company must notify the Norwegian Data Protection Authority within 72 hours. In addition, the individual(s) of the personal data must be notified with an explanation of what has happened, and actions taken to rectify the situation. Finally, *Article 37* instruct some companies have to assign a Data Protection Officer. A Data Protection Officer must have adequate knowledge about the laws and regulation, but does not have to be a lawyer *(Article 37, Clause 5)*. Typical chores are counselling and quality assurance of the organisation's personal data management.

3. RELATED RESEARCH

Albeit GDPR being relatively new, the topic has gained exponential interest from both researchers and industry since its formalised announcement on April 27th, 2016. However, it is worth remembering that GDPR is an extension of the «Lov om behandling av personopplysninger» as found in https://lovdata.no/dokument/NL/lov/2000-04-14-31 that was implemented January 1st, 2001 in Norway. (While it is not common practice to translate the name of Norwegian laws to English, we offer this unofficial translation to potential non-Norwegian readers as: «Law on process of personal data».) Consequently, we have included research of information privacy as well as GDPR.

We mainly used the AIS electronic library (requires subscription) and Google Scholar for conducting our search for related research. While we have focused on peer-reviewed publications, we also include some websites, bulletins, and other non-academic sources.

3.1 Information privacy

Existing research on information privacy is extensive and our point of departure was the comprehensive literature review provided by Bélanger and Crossler who studied more than 500 articles of information privacy research in information systems. Information privacy is a subset of privacy, and the latter concept dates back to 1890 when privacy was defined as "the right to be left alone" by Warren and Brandeis (Bélanger & Crossler, 2011).

Information privacy is usually referred to as only *privacy* in information systems research, as they apply continuity in the models associated with information privacy (Dinev, Xu, Smith, & Hart, 2013). It is worth to briefly mention the overlapping concepts such as security; anonymity; and secrecy, which has been added to the confusion of the information privacy concept. Security is often pitted against privacy, but instead of viewing them as concepts in conflict with each other, it should be recognized that they are mutually dependent on each other (The Norwegian Data Protection Authority, 2014). We will use these concepts interchangeably in this paper.

3.2 Company strategies for GDPR compliance, benefits and challenges

Colesky, Hoepman and Hillen (2016) present a critical analysis of privacy strategies, which amongst other consists of patterns. Based on their literature review they present an overview of nine patterns: Creating Privacy Policy, Fair Information Practices, Respecting Social Organizations, Appropriate Privacy Feedback, Maintaining Privacy Policy, Usage Control Infrastructure, Distributed Usage Control and Sticky Policies. From these patterns the authors derive eight strategies for organisations to comply with GDPR, as shown in Figure 1 below.

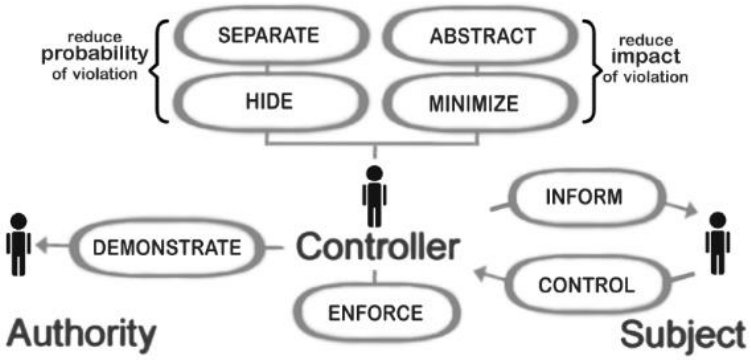

Figure 1. Strategies by data protection legislation actors (Colesky, Hoepman & Hillen, 2016, p. 39).

While Colesky et al. (2016) demonstrate a good overview of various concepts such as patterns, strategies and tactics pertaining to GDPR, there is no empirical evidence or insights of what companies find challenging. However, potential opportunities and challenges have gained interest in other research. As reported by Lomas (2016), the opportunities were fewer than the challenges, but one benefit typically dealt with cleaning up data. This meant both disposing data, and making data consistent. One of the greatest concerns was procedures around whistle-blowing (Lomas, 2016). Other potential benefits are that GDPR compliance can lead to satisfied customers and competitive advantage. An empirical study conducted by Kleindienst, Nüske, Rau, & Schmied (2017) revealed that customers will value companies who offer insights before the customers have asked for it; thus, they focus on benefits. Somewhat contradictory to other studies, the empirical paper by Crossler and Posey (2017) warns companies against using the individual's privacy concerns as promotion, although it might be tempting. Rather, Crossler and Posey suggest that developers and marketers should focus on the company's ability, benevolence and integrity. These three factors constitute a company's trustworthiness. *Article 17: The right to erasure* has gained much interest. For example, Mantelero points out that it is not anything new and can be traced back to Warren and Brandeis in 1890 (Mantelero, 2013) and Korenhof et al. discuss the many factors such as 'time' and how difficult it is to remove data posted on the Internet (Korenhof et al., 2015). Several researchers point to unwanted consequences such as identity theft (Solove, 2005) and the challenges of how this right should be handled in practice (Koops, 2011).

Several business reviews offer various advice on what companies need to do to become compliant. Examples typically include mapping of data and creating scenarios in order to be ready if an individual should demand access to data (Hyland, 2017). Finally, there are some publications on GDPR myths, and what the new regulation does not require. Two examples of *myths busters* read: (i) not all companies need a Data Protection Officer. It is only mandatory if the company is public, engage in monitoring, or handle sensitive data, and (ii) Individuals do not have the right to be completely forgotten. They can only claim this right if consent has not been given, or, data is being used for other purposes then first stipulated (Lee & Pickering, 2016).

3.3 Challenges with algorithms and explainable AI (Artificial Intelligence)

Goodman and Flaxman focus on algorithmic decision-making and Article 22: *the right to explanation*. Algorithms are perceived as objective, but if the training data set contains discrimination, biased decisions will be reproduced. Their main argument is that GDPR may pose large challenges for industry, but that it will also give computer scientists the opportunity to design better algorithms that will avoid discrimination and enable explanation (Goodman & Flaxman, 2016). According to Burrell there are

three main barriers to explainable algorithms: (i) The organisation intentionally conceals the decision making procedures from the public; (ii) most people are technical illiterate, which mean that, having access to the algorithmic code is insufficient; and (iii) a *''mismatch between the mathematical optimization in high-dimensionality characteristic of machine learning and the demands of human-scale reasoning and styles of interpretation''* (Burrell, 2016 p. 2). Our interpretation of this last barrier is that the public must have insights to both the training data as well as the algorithmic code. From Goodman and Flaxman study we conclude that both algorithms and humans are subject to discriminations. The viewpoint is mirrored in Koops and Leenes, with the argument "*Privacy Regulation Cannot Be Hardcoded"* (p. 1), rather it rests in the mind-set of the developers and people who interact with information systems (Koops & Leenes, 2014). Their paper mainly addresses Article 23 *Data protection by design and by default* – or more commonly referred to as *Privacy by Design*. Koops and Leenes have a specific call for further research that embrace both technical and organisational measures.

3.4 Summing up the related research

We found that the related research tends to be either from a legislation view (such as describing GDPR and the consequences for neglecting to comply), or, from a technological view (for example how algorithms and machine learning work). One of the conclusions it that research on information privacy has been focusing on the individual and there is a call for more research on privacy at the organisational level (Bélanger & Crossler, 2011). In addition, we noted that there is more focus on the challenges and obstacles than there are of the potential positive consequences of GDPR.

4. METHOD

Due to the fact that GDPR is a relatively new topic, this is an explorative study that aims to identify some insights and descriptions of organisational compliance. While several non-academic surveys as well as academic publications have painted a rather bleak picture and concluded that companies will not be ready on time, or, that they will face severe challenges after May 25th, 2018, we wanted to focus on companies that were somewhat aware of GDPR and in the process of becoming compliant.

As presented in Section 2, we started by studying the 99 articles of GDPR as found on the official website (https://gdpr-info.eu/). We also consulted this website (https://www.eugdpr.org/). Having identified eleven articles that we argue will have most impact on companies' information systems and management, we developed and conducted an online survey. Along with this, one of the researchers participated in one ongoing GDPR project in one large Norwegian company. Section 4.1 describes how the online survey was conducted, while Section 4.2 explains how one member of the research team participated in a GDPR project.

4.1 Online survey questionnaire

We developed an online questionnaire consisting of ten background questions and nine survey questions (in the form of statements). The answer alternatives in the survey were a combination of Likert-scale, multiple choices and open-ended comments (qualitative answers). We also strived for a simple and user-friendly design of the survey. The questionnaire was administered through the software tool SurveyMonkey® and the data were collected through a Web-link created by the software. We provided an introductory text where the purpose of the study was clearly communicated, in addition to who in the company we wanted to answer the survey; namely an employee in the company's management/administration department.

Prior to the distribution, the research team discussed the survey in detail, as well as completing several pilot tests, which resulted in a few modifications and changes to the questionnaire. Moreover, we clearly informed about the subject of the investigation, data processing, the purpose of the study and the rights of participants. We also informed that the answers are being processed according to the guidelines from the Norwegian Centre for Research Data (http://www.nsd.uib.no/). Average time for completing the survey was 6 minutes (reported by the survey tool). This was in line with the time (minutes) that the participants were predicted in advance.

Our survey was distributed to Norwegian companies from December 2017 to March 2018, mainly when we attended seminars about GDPR. In addition, the Norwegian Computer Society (Den Norske Dataforeningen) sent our survey link via e-mail to their professional network consisting of about 700

Norwegian companies. The survey was closed after 62 useful respondents had completed the questionnaire. But, we emphasise that not all the respondents answered every question, because some of the questions were not mandatory to complete the survey.

Survey Respondents Profile (N=62)	
Sector	Public: 26%
	Private: 74%
Number of employees in the company	10 employees or fewer: 8%
	11-20 employees: 10%
	21-50 employees: 5%
	51-100 employees: 7%
	101-300 employees: 16%
	301-600 employees: 16%
	Over 600 employees: 38%

Table 1. Overview of the respondents included in the study.

As we can see in Table 1 above, the majority of our participants were from the private sector and belonging to a large company with more than 600 employees (represented by 38% of the respondents).

4.2 Participation in one GDPR Project

One of the researchers followed a GDPR project in one large company, of which has to be kept anonymous. Consequently, we refer to it as 'the case company'. The case company was situated in Norway with offices in three cities. The researcher was technical consultant and reported directly to the project manager. While we acknowledge that this company was selected as a matter of convenience (Oates, 2006), it is nonetheless interesting because it had an ongoing GDPR project. The case company had started the project in November 2017. At the time of submission of this paper, the project was considered successful in the sense that it had a solid foundation in the top management; it had a project champion (who was also the project manager); and it involved the end-users. The case company was in the process of informing all departments and putting the employees to work in mapping data and business processes. A Data Protection Officer had been assigned and attended many of the information meetings. Our research approach was to simply observe and take notes during meetings and workshops. The notes were approved by the project manager prior to the submission of this paper.

5. FINDINGS AND DISCUSSION

This section is structured in five topics (sub-sections). Under each section we first present the findings from the survey questionnaire, followed by our observations from the GDPR project. Our findings are then briefly discussed against existing research.

5.1 General awareness

From Table 2 we note that our findings are, overall, less bleak than some of the existing research that are presented in Section 3. 57% has prioritised GDPR during the last year (2017), and 45% claim to have great knowledge about it. One explanation can simply be that our survey was sent out closer to the implementation date (May 25th, 2018) then previous surveys, but also that some of our participants were reached by means of The Norwegian Computer Society who have been arranging several seminars on GDPR. Since our aim was to focus on companies that had some awareness of GDPR, we consider this to be in line with our expectations.

Our observations of the case company were consistent with the findings from the survey. Again, since we had deliberately chosen a company that has started a GDPR project, we were not surprised by this result. However, in the case company, it was rather the managers of each department that were familiar with GDPR. Quite a few of the end-users/other employees admitted that they had never heard of it before the information meetings. We found that some of the existing research tend to focus on rights for the consumer, and thus neglecting the employees in a company. For example, Kleindienst et al. (2017) suggest that companies should reveal the identity of the employees that handle customer's data. This makes us question the privacy of the employees! The case company specifically stated that GDPR comprised: employees/owners, vendors/suppliers, customers/prospective. In addition, these three groups had three states: existing, past, and future. We observed that some of the participants were

reluctant to attend the information meetings, but became interested when they understood that they, in the role of employees, possessed both rights and responsibilities. Colesky, Hoepman and Hillen (2016) simply refer to these groups as "Subjects" in Figure 1, but our findings reveal a lot more details.

To what extent has GDPR been a topic in the company during the last year? (N=61)	
GDPR has been a priority topic	57%
GDPR has been a topic on a regular basis	25%
There has been a topic, but not often	8%
GDPR has rarely or never been mentioned	5%
Do not know	5%
To what extent does the company know about GDPR? (N=50)	
Do not know at all	6%
Have heard about it	6%
Have heard about it, but it seems difficult to understand	8%
Have great knowledge about it	45%
Know it very well and all that matters to the company	35%
Do not know	0%
Does the company have a Data Protection Officer? (N=51)	
No, we are not required to have it	27%
No, but we will within the deadline	20%
Yes, and we are required to have it	31%
Yes, but we are not required to have it	12%
Do not know	10%

Table 2. General awareness of our companies in the survey.

5.2 Preparation for the new regulation

Table 3 explores the preparation in more detail. Again, we note that the majority of the participants are well prepared regarding issues within the organisation.

To what extent the companies are prepared for new regulations (N=50)						
	Completely disagree	Disagree	Medium	Agree	Completely agree	Do not know
Familiar with the regulations	4%	6%	12%	34%	42%	2%
Control of data for insights or deletion	6%	2%	12%	48%	22%	10%
Good IT solutions	6%	12%	28%	24%	24%	6%
Adequate competence	2%	20%	16%	40%	20%	2%
Adequate resources and training	4%	24%	34%	22%	14%	2%
Routines for reporting data breach	8%	20%	22%	20%	24%	6%
Prepared for data portability	8%	22%	24%	24%	14%	8%

Table 3. To what extent the participants are prepared for the new regulations.

The case company demonstrated maturity on many issues. For example, it was decided that the project manager and the technical consultant (the researcher) should give an information meeting to every department, and in every city. It was constantly repeated that no short cuts were to be taken. Consequently, a presentation was created with an introduction of the same eleven articles as presented in this paper, and tangible suggestions of what had to be done. All participants were given two tasks: map what kind of data they handle, and where the data are stored. They were given a quick introduction to Business Process Management Notation (BPMN) as found on Wikipedia (https://en.wikipedia.org/wiki/Business_Process_Model_and_Notation) with instructions to use only the simplest notations. They were also instructed to create scenarios and perform risk analysis (also known as Data Protection Impact Assessment (DPIA), which is defined in *Article 32* in GDPR (The Norwegian Data Protection Authority, 2018)). For example, the project manager painted two scenarios: *"We have an e-mail from a customer, asking about data portability", and "We have a furious customer at the front desk, claiming that we have not erased her personal data." In both cases: What do we do, and who is in charge?* The project was still ongoing at the time of submitting this paper so unfortunately, we do not know the results of this mapping.

5.3 Articles of the greatest concern

Based on the eleven articles that the study considers relevant to Information systems, respondents were asked to tick off the articles of the greatest concern. They could tick off all articles that applied to them. Table 4 reveals the top three concerns, which are *Article 17: The right to erasure ("be forgotten")*, *Article 30: Records for processing activities*, and *Article 25: Data protection by design and default*. At the bottom we find *Article 37: the designation of the Data Protection Officer*. 25% stated "Do not know/not applicable to our company", and two participants shared their comments related to this. They both stated that they *"do not handle much personal data in our company"*. We are unsure how to interpret the somewhat high percentage that ticket off "Do not know/not applicable to our company". It seems to be a mismatch between the claims in Table 3, where the majority agree, or completely agree, to be *familiar with the regulations*. Of course, the regulation consists of more than these eleven articles, and, indeed, GDPR does not apply to companies that are completely detached from EU. Since we lack full control over the nationalities of our participants, this can be one explanation.

Articles that are of greatest concern (N=48)		
Article 17	Right to erasure ("be forgotten")	42%
Article 30	Records of processing activities	31%
Article 25	Data protection by design and by default	29%
Article 7	Conditions for consent	25%
Article 5	Processing of personal data	23%
Article 15	Rights of access	21%
Article 20	Right to data portability	21%
Article 22	Automated decision-making	19%
Article 32	Security of processing	19%
Article 33	Notification of a personal data breach	19%
Article 37	Designation of the Data Protection Officer	4%
	Do not know/not applicable to our company	25%
	Other	4%

Table 4. Articles of the greatest concern

During the observations in the case company, *Article 37* was almost disregarded, since a Data Protection Officer had been assigned. However, not all employees were aware of what this role actually meant and how they could benefit from it. The Data Protection Officer himself said: *"Many employees have the (wrong) impression that I alone have the responsibility to initiate and manage routines and processes for data management in all departments. I have also experienced that my role has been wrongfully perceived as an alibi for GDPR compliance in this organisation."* We have not found any previous studies that have mapped the articles in the same manner that we have, but our participants clearly place *Article 17: the right to erasure ("be forgotten")* as the top challenge. This challenge is congruent with existing research, especially the critical analysis by Koops (2011).

5.4 Other challenges and opportunities

On the question of which challenges the company faces when introducing GDPR, 23% lacks budget and 18% lack of required technology. About 46% of respondents reply that they have a limited understanding of GDPR, and 44% have also faced other challenges. Some of the comments read: *"The amount of work and activity remaining"*, *"clarity of the text (regulations) itself"* and *"lack of resources"*.

Furthermore, our survey also focused on the benefits of introducing GDPR and 33% believed that this was a competitive advantage for the company. 51% responded that there was a way to clear old data while 60% of this would lead to changes in procedures and routines. Additional comments from the respondents regarding GDPR and consequences included a blend of positivism and confusion:
"It is positive for the users, but the regulations are too general."
"The public sector is unprepared for the change."
"Important direction to take care of your privacy. This is only the beginning of the journey, not a goal to be reached."

From our observations during the GDPR project, we noted that the case company was very positive towards the new regulations, and they typically stated that it would be nice to make a total cleaning of

digital data, physical documents, various systems, e-mail attachments and more. At one point the project manager at the case company pondered: *"This project is going surprisingly well. Almost too well. Are we overlooking something?!"*. However, some of the participant of the information meetings demonstrated frustration and re-occurring comments were: *"So, I cannot have any spreadsheets on my own computer?"* and *"Do I have to delete all of my e-mail correspondence now?"* The project manager, along with the technical consultant (the researcher) and the Data Protection Officer provided answers on the spot, which proved to be worth the time spent. (The answers to such questions have too many conditions and prerequisites that we dare to provide a general response in this paper. However, a company can come a long way by (i) *justifying* the *reason* for *why* they keep the spreadsheets and e-mails, and (ii) that they are *secured* in *the best possible manner*.) In addition, Article 6 instructs that companies must demonstrate that they are possessing personal data affected by GDPR. This means that if the spreadsheets and e-mails do not contain personal data as explained in our introduction (and grounded in *Article 4*), they are not comprised by GDPR. Again, these findings do to a large extent confirm existing research, such as Koops (2011) and Koops & Leenes (2014) regarding challenges, as well as Lomas (2016) when it comes to benefits.

5.5 Financial sanctions

The compliance of GDPR is mandatory for companies, unlike, for example, the implementation of a new information system such as ERP or CRM. Similarly, the potential high fines are probably unfamiliar challenges. Failing to comply with the regulations concerning GDPR might result in financial consequences for the companies. However, The Norwegian Data Protection Authority will give advises and recommendations before taking such an action, but this is an authority they have if it is needed. One of the questions in the survey was therefore linked to financial sanctions businesses may receive if they do not comply with current regulations and/or follow advises from The Norwegian Data Protection Authority.

Respondents were asked to calculate their size, which can reach up to 4% of global sales, or 20 million Euro, whichever is higher. 36 respondents provided an answer to this question, but only 19 of these were in concrete amounts in either Norwegian Kroner (Crowns) or Euro (respondents who did not specify the currency, only the amount, were excluded from the average estimates). Beyond this, two participants wrote: *"Yes, but will not give up"* and *"Difficult to calculate the amount"*. Another comment read: *«I do not understand how to calculate this fine. It reads: "up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher". How this could ever be more than €20 million is beyond my comprehension."* However, the fine can indeed be above €20 million. We also suspect that some of the respondents who answered "20 million Euro" believe that this is the maximum fine. Our findings reveal that the highest amount among the respondents is €1 666 892 392 and the lowest amount is calculated to be €400. These results demonstrate large differences, both in terms of revenue and economic consequences for individual companies. The mean amount among the respondents is €628 546 751, while the median is €5 200 000. As we can see, for some companies, such sanctions will result in significant financial consequences.

From the observations from the case company, the rules of financial sanctions were presented at every meeting, but surprisingly little concern was paid to this aspect. Some laughter was observed, along with humorous comments on what the Norwegian Data Protection Authority was going to do with the money from potential fines: *"They will have nice Christmas parties"*. Then they quickly focused on the potential benefits and were more concerned about compliance within the deadline.

5.6 Summing up findings and discussion

Summing up this section, we offer the following insights. First, virtually all European companies must comply with GDPR. Even companies that do not handle personal data about customers will most likely have data about employees or suppliers, both from the past, current and future. The new regulation also influences a company's website. Second, unlike for example the decision to implement an ERP- or CRM system, GDPR compliance is compulsory, and the financial sanctions are substantial. From the case company, we observed that the project had quite a traditional character with strong top management foundation. Unfortunately, our data does not allow us to draw any conclusions about how GDPR-related projects should be handled in the future. However, it should not be necessary to re-invent the wheel. As

argued for example by Solove (2006) and Mantelero (2013) information privacy is not something new, and we have argued that Norway has had a strict law prior to GDPR. From the case company we noted that they followed some long-existing success factors from IS research: they had started with gaining a solid foundation from the top management; they banned short-cuts; they did not believe that purchasing new technology alone would solve the challenges; they focused on low-hanging fruits (benefits).

Table 5 summarises our identified challenges and opportunities, mainly from a managerial perspective. We acknowledge that the level is abstract and lacks tangible details, however Table 5 is based on both existing research and our empirical data. We argue that complying with GDPR is mainly a managerial responsibility, but virtually every individual in the organisation must be informed.

Challenges	***Our advice in a GDPR context***	***Comments***
1) Understanding the regulation and the consequences.	- Assign responsibility to roles. - Compliance must be reflected in contracts, culture, and more. - Employee trainings. - Procedures for whistle blowing.	- Mainly a management task. - We offer eleven articles as a starting point (see the Appendix).
2) Which data does the company possess, where are the data stored, and who has access?	- Workshops; mapping data and business processes by using the essential BPMN symbols. - Create possible scenarios. - Perform risk analysis (DPIA).	- Employees together with manager of every department. - Use the how-to's from the Norwegian Data Protection Authority (2018[b]).
3) Do we need new technology?	- If deemed necessary, purchase new technology, but after the mapping.	- Collaboration between IT department and management.
Opportunities	***Our advice in a GDPR context***	***Comments***
1) Cleaning data (digital and physical) and simplifying business processes.	- See challenge number 2). - Aim for transparency. - Focus on long-term value.	- Employees together with manager of every department.
2) Creating good reputation and competitive advantage for the organisation.	- Can backfire if only empty words and not reflected in the company's actions. - Quiz for all employees; new and existing.	- Mainly a management focus, but the whole organisation should be obliged to follow established guidelines.

Table 5. Our identified challenges and opportunities when complying with GDPR.

5.7 Limitations and suggested further research

We acknowledge that our study has several limitations, but some of these are opportunities for future research. First, the questions in our survey were on a superior level and made it difficult to collect detailed information. Second, we also acknowledge that some of our survey questions could be misunderstood. Third, we have to disclaim any legal aspect – although we have tried to address both law and technology in this paper, all of the three authors of this paper have a technical background. Fourth, although we have carefully selected eleven articles for this paper, it does not mean that the other 88 articles should be excluded from information systems research. As such, we suggest a research team with both technologists and lawyers. Finally, we acknowledge that our identified challenges and benefits are abstract and lack tangible, detailed advice. Future research can therefore identify and create software engineering patterns (Larman, 2005), that is, problem-solving pairs to re-occurring issues in a company.

6. CONCLUSION

The aim of this explorative paper was to identify and describe opportunities and challenges that Norwegian companies face when complying with the EU's General Data Protection Regulation (GDPR).

Our findings indicate that at the time of our data collection (spring 2018), Norwegian companies state to have more challenges than opportunities, but they are in the process of overcoming the challenges. They struggle with understanding the regulation, such as the financial sanctions. The highest fine stipulated by our respondents amounted to €1 666 892 392 (almost 1,7 billion Euro) – in other words, a considerable amount of money! Related to the 99 articles that constitute GDPR, three articles were of particular concern: *Article 17: The right to erasure,* (also known as *"the right to be forgotten"*), followed

by *Article 30: Records of processing activities* and *Article 25: Data protection by design and default*. We also noted some positive attitude towards the new regulation. Opportunities typically included a chance to clean and gain control over the vast amount of data in a company, as well as demonstrating trustworthiness to their customers.

Our contribution is mainly to the industry. We present eleven articles as a starting point (found in Section 2 and the Appendix), along with a list of identified challenges and opportunities (see Table 5). Our contribution to academia is small, but we argue that complying with GDPR is interesting for several future research projects within the Information Systems field. For example, we argue that it should not be necessary to re-invent the wheel when complying with GDPR and that there exist many models and theories within Information Systems than can be applied.

Acknowledgements
We thank all participants who provided answers to our survey, as well as The Norwegian Computer Society (Den Norske Dataforeningen) who helped distributing the survey via e-mail. Gratitude goes to Atea who granted us first-hand access to their collected data, and Pål E. Wæraas and Knut Erik Gaustad for comments. Last, but not least, we thank the anonymous NOKOBIT reviewers for useful feedback.

REFERENCES

Arbeidsnytt (2018) https://arbeidsnytt.no/gdpr/gdpr-datatilsynet-har-fatt-en-ny-svaer-revolver-i-beltet-sier-fjortoft/100274 (Accessed date: 27.02.2018).

Bark, O. N. (2017). GDPR - et hav av muligheter gjennom kontroll. En undersøke av Atea. *Presented at The Norwegian Computer Society seminar on January 16th, 2017*.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly, 35*(4), pp. 1017-1041.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), pp. 1-12.

Colesky, M., Hoepman, J.-H., & Hillen, C. (2016). A critical analysis of privacy design strategies. *Paper presented at the Security and Privacy Workshops (SPW)*, 2016 IEEE.

Crossler, R. E., & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems, 18*(7), pp. 487-515.

Davenport, T. H., & Kirby, J. (2016). *Only humans need apply: winners and losers in the Age of smart machines*: HarperCollins Publishers.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems, 22*(3), pp. 295-316.

European Parliament (2016) Data protection reform - Parliament approves new rules fit for the digital era. http://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era (Accessed date: 14.04.2018)

Goodman, B., & Flaxman, S. (2016). European Union regulations on algorithmic decision-making and a "right to explanation". *arXiv preprint arXiv:1606.08813*. pp. 1-10.

Hyland, J. (2017). Data Protection in EU Businesses: an Introduction to GDPR. *DBS Business Review*, pp. 146-148.

Justis- og beredskapsdepartementet (2017) Høringsnotat: Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett. Available at: https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat--ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett.pdf (Accessed date: 14.04.2018)

Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2017). Beyond Mere Compliance - Delighting Customers by Implementing Data Privacy Measures? . *in Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen*, pp. 807-821.

Koops, B.-J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice. *SCRIPTed, 8*, pp. 229-256.

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. *International Review of Law, Computers & Technology, 28*(2), pp. 159-171.

Korenhof, P., Ausloos, J., Szekely, I., Ambrose, M., Sartor, G., & Leenes, R. (2015). Timing the right to be forgotten: A study into "time" as a factor in deciding about retention or erasure of data *Reforming European data protection law*. Springer, pp. 171-201.

Larman, C. (2005). *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development (3rd Edition)*: Pearson Education, Inc.

Lee, P., & Pickering, K. (2016). The general data protection regulation: A myth-buster. *Journal of Data Protection & Privacy*, 1(1), pp. 1-5.

Lomas, E. (2016). Data Protection and GDPR Opportunites and Challenges. *IRMS London Particpatory workshop hosted by UCL, 7 July 2016.*, pp. 1-6.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review, 29*(3), pp. 229-235.

The Norwegian Data Protection Authority (2014). Personvern. Tilstand og Trender 2014. *Available at:https://www.datatilsynet.no/globalassets/global/04_planer_rapporter/persovern_tilstandog trender_2014.pdf* (Accessed 16 December 2015).

The Norwegian Data Protection Authority (2018[a]) https://www.datatilsynet.no/en/about-privacy/reports-on-specific-subjects/ai-and-privacy/ (Accessed date: 27.02.2018).

The Norwegian Data Protection Authority (2018[b]) https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/?id=10365 (Accessed date: 02.08.2018).

The Norwegian Data Protection Authority (n/d) Guide. Software development with Data Protection by Design and by Default. (https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/) (Accessed date: 14.04.2018).

Martin, K. E. (2015). Ethical issues in the big data industry. *MIS Quarterly Executive, 14*(2), pp. 67-85.

Oates, B. J. (2006). *Researching Information Systems and Computing*: Sage Publications Ltd.

Rightbrain (2018) https://rightbrain.no/gdpr-storste-endring-pa-20-ar/ (Accessed date: 27.02.2018).

Presthus, W., & Andersen, L. (2017). *Information Privacy from a Retail Management Perspective.* Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017. pp. 1968-1983.

Presthus, W., & Sørum, H. (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. *Accepted for Procedia Computer Science*.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154, pp. 477-560.

APPENDIX: DETAILED PRESENTATION OF SELECTED ARTICLES FROM GDPR

This appendix is based on three main references (see below), but we have used our own words in order to demonstrate how the articles apply in an information systems' context for a company. Please note that a **controller** decides what purpose the data is being collected for, and how, it is being collected. A **processor** only performs the processing on behalf of, and under instruction from, some other organisation.

Article 5: Principles relating to processing of personal data
Personal data shall be processed with fairness, lawfulness and transparency in relation to the individual, and only collected for specified, legitimate and explicit purposes. It is also applying to every personal data processing activity, and should be kept in mind when interpreting the rights and duties in GDPR. (This includes the principles of *data minimisation*, *integrity*, *accuracy*, and *accountability*.)

Article 7: Conditions for consent
The individual shall have the right to withdraw his or her consent at any time and it shall also be as easy to withdraw as give consent. The controller shall be able to demonstrate that the individual has consented to processing of his or her personal data and it shall be freely given.

Article 15: Rights of access by the data subject
The individual shall have the right to obtain confirmation to whether or not personal data concerning him or her is are being processed. Where that is the case, him or her also have the right to obtain the purpose of the processing, categories of personal data concerned, the recipients of their personal data (in particular third countries or international organisations) and be provided a copy of the personal data undergoing processing.

Article 17: Right to erasure ("right to be forgotten")
The individual has the right to obtain erasure from the data controller, without undue delay if one of the following applies:

- The controller does not need the data anymore.
- The individual withdraws consent for the processing with which they previously agreed to and the controller does not need to legally keep it (but many will, e.g. banks need to store for 7 years).
- The individual uses their right to object (Article 21) to the data processing.
- The controller and/or its processor is processing the data unlawfully.
- There is a legal requirement for the data to be erased.
- The individual was a child at the time of collection (Article 8 have more details on a child's ability to consent).

Article 20: Right to data portability
The individual shall have the right to receive their personal data concerning him or her, which he or she has provided to a controller, and reuse it for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Article 22: Automated individual decision-making, including profiling
The individual shall have the right to not be subject to a decision based solely on automated processing (without any human involvement) including profiling (automated processing of personal data to evaluate certain things about an individual).

Article 25: Data protection by design and by default
The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are

processed. Privacy by design has always been an implicit requirement of data protection which the Norwegian Data Protection Authority has recommended.

Article 30: Records of processing activities
Each controller, where applicable, shall maintain a record of processing activities under its responsibility. It shall contain the following:
- The name and contact details of the controller, joint controller, data protection officer and controller's representative.
- Purpose of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipient to whom the personal data have been or will be disclosed to.
- Transfers to third country or international organisations.
- Technical and organizational security measures referred to in Article 32 (Security of processing).

Article 32: Security of processing
- Identify the scope of the assessment and assets (the nature, scope, context and purposes of processing)
- Perform a risk assessment is performed (the risk of varying likelihood and severity for the rights and freedoms of natural persons).
- Finally review the risks, and decide on the risk treatment (taking into account the state of the art, the costs of implementation). The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to risk.

Article 33: Notification of a personal data breach to the supervisory authority
In the case of personal data breach, the controller shall without undue delay, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority. Unless, the personal data breach is unlikely to result in risk to the rights and freedoms of natural persons.

Article 37: Designation of the Data Protection Officer
The controller and the processor shall designate a Data Protection Officer in any case where:
- They are a public authority (except for courts acting in their judicial capacity).
- There is carried out large scale systematic monitoring of individuals (for example online behaviour tracking).
- There is carried out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size. Any organisation is able to appoint a Data Protection Officer. Regardless of whether the GDPR obliges you to appoint a Data Protection Officer, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

References used in describing the articles:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
https://gdpr-info.eu/
https://www.linkedin.com/pulse/practical-use-gdpr-article-32-security-processing-carsten-jorgensen/