UiO : Department of Informatics
University of Oslo

T149 - How GDPR changes business

INF3510

15320, 15125, 15354

Contents

1 Abstract, motivation and introduction

1.1 Abstract

In this research paper we will show how the General Data Protection Regulation (GDPR) affects consumers, businesses, developers and their project workflow. Through interviews, analysis of literature and current business guidelines, we have created a framework for implementing GDPR and privacy in general in a business.

1.2 Motivation

GDPR is going to impact a lot of companies. Having knowledge about, and being aware of the rights of data subjects and potential penalties for not following the regulation is important. Considering that we in the future most likely will be working in the IT industry, we will stumble across GDPR in some way. In addition to being interested in privacy and the EU, this was a deciding factor when were to choose what to write about.

1.3 Introduction

The GDPR will be in effect from the 25th of May 2018. It's an initiative to uniform and improve privacy laws across the EU. This research paper will first of all give an introduction to GDPR, its history and its content. What follows is our own research, done both online and by interviewing norwegian companies about their GDPR implementation. We will then summarize the key elements from our research in a framework that can be used when implementing both privacy in general and GDPR in a company.

2 The basics of GDPR

When figuring out the basics of GDPR, we started by looking into relevant articles published by both law firms and IT companies. We gathered key points into a list - and then began researching each element. This quickly lead us to the law itself.

2.1 The history and timeline of GDPR

The European Data Protection Directive was adopted in 1995. This directive included the seven principles that The Organisation for Economic Co-operation and Development (OECD) proposed in 1980 in their "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data". In 2011 the European Data Protection Supervisor published an Opinion on the European Commission's Communication. An Opinion is in this case a draft to either improve or implement a law or a guideline. In January 2012 The European Commission proposed a comprehensive reform of Directive 95/46/EC to improve online privacy rights and boost Europe's digital economy, which was the starting point of GDPR. Two months later, the European Data Protection Supervisor adopts an Opinion on the Commission's data protection reform package. The Article 29 Working Party (a working group made up of each data protection authority - like "Datatilsynet") adopts an Opinion on the data protection reform proposal shortly after. This means that the relevant parties agreed on improving privacy across the EU, and sent the draft to the European parliament.

In 2014 the European Parliament votes in favor of the GDPR with 621 votes in favor, 10 against and 22 abstentions. In 2015 the European Data Protection Supervisor publishes his recommendations which is then discussed by the European co-legislators in the form of drafting suggestions. They all reached an agreement in December 2015. From 25th of May 2018 the regulation will apply, two years after the regulation entered into force. [1]

The General Data Protection Regulation is a regulation made by the European Parliament and Council of the European Union with the goal of enhancing data protection rights of individuals and to improve business op-

portunities by facilitating the free flow of personal data in the digital single market. [2]

It will replace Directive 95/46/EC, by adding new principles such as requirement for data portability, "the right to be forgotten" as well as a stricter concept of consent. As a regulation, the GDPR will have direct legal effect throughout the EU, enforced by national data protection authorities and courts. This means that it doesn't require transposition into national legislation - which in turn secures uniformity in standards and interpretations across Europe. [3]

GPDR was introduced because the EU wanted to give people control of their own data and how it's being used. Keep in mind that Directive 95/46/EC was made before the Internet and Cloud era, and thus wasn't up to date with how technology has changed in the last 20 years. EU also wanted to make it easier for businesses throughout Europe to operate cross borders by having one, uniform regulation. The EU estimates that this will save businesses overall by as much as €2.3 billion a year. [4]

As Norway is a member of the European Economic Area (EEA), it has to implement the Law of the European Union. [5] Norway does not have the right to veto a law in the EU, but the norwegian parliament can use the Reservation Right in order to deny making the EU law a law in Norway. No party in Norway has proposed using the Reservation Right to avoid making GDPR norwegian law. [6]

Although the law will apply in the EU on 25th of May 2018, the norwegian justice department has stated that the implementation might be postponed because of the EEA draft resolution to the EU. According to Rett24, the law is postponed to 1st of July 2018.[7]

If the implementation is postponed, the EU and norwegian privacy rights will differ, contrary to what the law was intended to resolve. This isn't a pressing matter because Norway has implemented their own privacy laws, that on many areas are similar to the GDPR. [8]

Some key differences between the GDPR and current norwegian law are that all businesses and organisations have new duties in regards to privacy and risk assessment. Businesses are also required to have an understandable privacy policy, and the implementation of Privacy by Design. Some businesses also need to have a Data Protection Officer, and their data handlers have new

duties. These, and many more changes will be discussed further in this research paper.

2.2 Contents of the law

2.2.1 Data breaches

GDPR introduces new rules regarding data breaches. Breach notification will be mandatory in all countries where a data breach is likely to "result in a risk for the rights and freedoms of individuals". Within 72 hours after a data breach has been discovered, the company has to notify the local data protection entity. Article 33 states that data processors will be required to notify their controllers and customers "without undue delay" after the data breach is first known. [9]

2.2.2 Right to access

As outlined by the GDPR, one of the rights the data subjects has is to obtain confirmation about where and for what purpose their personal data is processed. The data controller shall further provide a copy of the data, in an electronic format, free of charge. Considering data transparency and empowerment of the data subjects, this change is quite a dramatic shift. [10]

2.2.3 Right to be forgotten

The right to be forgotten, also known as Data Erasure, entitles the data subject to have the data controller delete his/her personal data, preventing any further processing of said data. The conditions for erasure is defined in article 17. It states that if the data is no longer of relevant use for the original purposes for processing, or if a data subject withdraws his/her consent then the data has to be deleted. [11]

2.2.4 Data portability

One of the new things being introduced by the GDPR is data portability - the right for a data subject to receive any personal data concerning them. This data has to be provided to a controller in a structured, 'commonly used and machine-readable format'. The subject also has the the right to transmit that data to another controller. [12]

2.2.5 Privacy by design

As a concept that has existed for years now, privacy by design is just now becoming a legal requirement with the GDPR. In short terms, privacy by design calls for the inclusion of data protection from the very beginning of the designing of systems. As stated in article 23, it calls for controllers to hold and process only a bare minimum so that only the data that is absolutely necessary for the completion of its duties is being used (data minimisation). [13]

2.2.6 Data protection officer (DPO)

The data protection officer serves an important role. One of the DPO's tasks is to inform and advise the controller or the processor, and the employees who carry out processing. The DPO must also provide training of the staff involved in processing operations, raise awareness amongst employees and monitor compliance with the regulation. The competent will act as a contact point for, and cooperate with the supervisory authority on issues relating to processing. The DPO is similar to a compliance officer and is also expected to be managing IT-services, dealing with cyber attacks and similar processes regarding data security. Other tasks are critical business continuity issues around the processing and holding of personal and sensitive data. The skill set that is required for this stretches beyond basic understanding of laws, regulations and legal compliance. [14]

2.2.7 Penalties for non-compliance

One of the mildest sanctions for cases of first and unintentional noncompliance is a written warning. Another rather mild sanction that can be imposed is regular periodic data protection audits. For worse and more serious noncompliance, the business must pay a fine up to €20 million or 4% of annual turnover. This is the maximum fine that can be imposed, and is imposed on more serious violations of the regulation, like not having sufficient customer consent for data processing or violating the core concepts of Privacy of Design. However, there is a tiered approach which is a fine up to €10 million or 2% of annual turnover. This could be because the business does not have their records in order or if the business is failing to notify supervising authorities about data breaches. [15]

2.2.8 Lawful basis for processing

The data collected can only be processed if there is at least one lawful basis to do so. There are six lawful bases that underlies here. Most important, consent from the data subject or that the processing is necessary for the performance of a contract. [16]

2.2.9 Consent

If the lawful basis for processing of collected data is consent, then the consent must be explicit. The purpose for collection of data and what the data is going to be used for must be such that the person giving consent understands and agrees to the terms. The consent for children is given by the child's parents or guardian. There has to be a way to prove that the consent is being given by the child's actual parents or guardian if that is the case. Consent can at any time be withdrawn if the person wishes to do so. [17]

2.2.10 Pseudonymisation

Pseudonymisation is when you have a set of data about a person and process it in such a way that you cannot identify the data to a specific data

subject with that information. The information needed to personalise the data is saved separately from the pseudonymised data for security reasons. There are two examples of pseudonymisation, the most common is encryption. Encryption is when you processes the data to unintelligible data. The key needed for decrypting the data is stored separately. The other example of pseudonymisation is tokenization. This method is non-mathematical and uses less space and processing power than encryption. The sensitive data is replaced with substitute data which is non-sensitive. Since the tokenization only substitutes the data, the size of the data is more manageable and can be processed easily by databases.

GDPR does not directly say that you need pseudonymisation, but that it needs something similar. You cannot store personal data directly, but need some sort of pseudonymisation. [18]

2.2.11 Records of processing activities

The controller, or the controller's representative is responsible for having all records of processing activities on record. This includes all contact details of the controller (and/or joint controllers), the purpose of the processing done, categories of data subjects and personal data. If possible, the record shall also contain the time limits for erasure of the data categories and a description of the organisational and technical security measures used. The description of the security measures should include the pseudonymisation and encryption of personal data used if it is possible. The controller and processor should take steps to ensure that a person under their authority with access to personal data does not process the data except on instructions from the controller, or if the law requires him/her to do so. These steps should also be described. The processor(s) shall also maintain a record of all categories of processing activities carried out on behalf of a controller, containing name and contact details of the processor(s) and controllers that are in charge of the processor(s). If possible, a description of the technical and organisational security measures listed above should also be included. In circumstances of data transfers of personal data to third party countries or international organisations, all information about those transfers should be included in the record. [19]

2.3 What is not covered by GDPR?

Although GDPR covers a lot of privacy concerns, there are a few cases that is not covered by the new law. Lawful interception by a state or national security is not covered, as well as statistical and scientific analysis. Management of data about deceased persons are subject to national legislation, and the Regulation does not cover the processing of personal data which concerns legal persons. A legal person is an entity that has privileges and obligations, and has the right to enter into contracts, be sued and sue others - in many cases a firm or a government entity. GDPR does not go into detail about employer-employee relationship because there's already an EU law about the matter. The law does not cover processing of data by a natural person for purely personal or household activity. [26] [25] [27]

3 Research

In this assignment we chose to do much of our research by reaching out to developers and key personnel in businesses. This way we were able to do a thorough analysis and draw parallels between what companies do with what we found online.

3.1 Methods

When looking into what the leaders and management did to be GDPR compliant, we talked to three companies and did research online. We then analysed the different solutions the companies used, comparing the results with what our research online showed. The results are presented in 3.2.

For the implementation project itself, we talked to three project managers (PM) and one DPO - both by phone and mail. Two PMs and one DPO in larger companies with 100+ employees, in addition to a PM in a startup in Oslo. We then compared the results with what we found online. This is shown in 3.3.

Since we are future developers, we wanted to find out how GDPR would affect a developer's workflow. We talked to some developers in the companies we

reached out to, as well as developers in our own network. We asked them how GDPR changed their workflow, where they find information and also how they thought future developers would get information about GDPR. We compared the answers from the developers with what we found online. The results are presented in 3.4.

Regarding getting information about how customers are going to be affected, we couldn't use as much of the research from the different businesses we talked to. Therefore we had to do some extra research online. The different sources online turned out to have a lot of similarities in their analysis of how GDPR would impact the consumers. This is discussed in 3.5.

3.2 Leadership

According to Diligent Technologies Corporation (DTC), the board of directors must take leadership in making a corporation compliant with the GDPR. Furthermore they stress that the new rules require the directors and officers in a company to certify their compliance with the law. If they are not in compliance, management in the corporation can be held personally accountable, which is why this law so important for them. According to the report, most board members "... act as 'consumers' of metrics and information provided by the operating teams regarding cybersecurity solutions, and then accept those teams' assessments of the level of protection".[20] GDPR requires that the board and leaders change their current view of cybersecurity solutions.

Today, businesses have a lot of responsibilities in regards to IT security and the protection of data. Jøsang, Audun states that corporations must take responsibility, follow standards and current laws. If they don't, they'll risk going to jail, the company drops in value or lose the trust of the consumers. [21]

In regards to the leadership and management of a company, they have to set clear goals, and be able to test these goals. This matches what John Chambers, CEO of Cisco and John N. Stewart, CSTO of Cisco, are saying - cybersecurity must start at the top. They state that "CEOs need to be able to answer tough questions and prove that they are leading a security strategy that works through testing and explanation." It goes without saying that this applies for GDPR and data privacy as well. [22]

While this is a great start to corporations being aware of security concerns and take action to promote security and privacy, how do norwegian businesses use leadership to promote privacy and to be GDPR compliant?

A company we talked to that deals with HR and tech, initiated a project once GDPR became known. Their goal was to improve and edit their internal processes so they would comply with the new rules. They have also sent people in leader groups to seminars in order to learn more about the law. This makes for a good basis for improved attention regarding the new laws and how it will affect the company. In order to make sure the company is compliant, they contacted a law firm who specializes in the new law. In addition to this, the firm gathered information from the norwegian data protection authority, "Datatilsynet". One company, an international consultant agency, appointed a DPO although they were not obligated to have one. Complaints were made by the leader groups that the norwegian version of the law was produced too late, giving the companies little time to adapt.

3.3 Implementation Project

The leadership and management in a company might not do the actual work of implementing or editing processes to be GDPR compliant. In our research we've found that companies usually assigns a group of people within the company to do project management. Some also hire external help, like the companies we talked about in 3.2. The members of this project are then tasked with finding out more about GDPR and which changes are relevant to the company.

Most companies that we have talked to and read about begins an implementation project by setting a budget, raise awareness and create a task force. Some leader groups do this themselves, or assign it to mid-level-management. After having initiated the project, they start data mapping. This means finding out what, where and the purpose of personal information and data processing within the company. In practical terms, this is being done by either gathering key personnel from different divisions inside the company to a workshop - or by sending out questionnaires that has to be filled out. Gathering information is done to achieve two goals. First off, it's done in order to create a basis for doing a gap analysis to find out what needs to be done by the company. In addition to this, it can be used when the company

is working on being compliant with Article 30 of GDPR, the requirement to record different types of data processing activities. [19]

After mapping out what information is used where, and where it's collected from, a gap analysis is performed. This is done by comparing the results from the data mapping phase with what the new law requires. Some frequent gaps are the lack of Privacy Impact Assessment, the data breach control and the implementation of a Data Protection Officer.

With the gap analysis finished, the company will have a clear list of tasks that has to be performed. For all the companies we talked to and read about, this is the most challenging and time-consuming phase. The companies will have to use the gap analysis and change current and future processes based on it. In practical terms this includes, but are not limited to, hiring and organizing a Data Protection Officer if needed, change how sensitive data is stored or change HTML forms to receive consents per GDPR law.

Furthermore the business could initiate other administrative measures to meet the requirements, such as preparing and documenting a privacy manual. With this, the business could easily look up the manual for a good overview of various important information, like procedures for processing data. This way the data protection officer can ensure compliance. The privacy manual is also helpful for employees when working with matters regarding personal data.

After the implementation phase is done, the companies we talked to stated that they will be ready for the new law. This process is similar to what Stibbe, an international law firm is recommending in their report about how to be GDPR compliant. [23]

3.4 Developers

When it comes to how developers are affected by the GDPR, we found several key points where they have to change their work habits.

As we have mentioned before, privacy by design & default is a big part of GDPR. The developers have to use this framework in current and future projects. One of the companies we talked to said that they have meetings with clients where they discuss projects to see if they need to adjust the code

or user experience. The workflow routines of the developers consists of more thorough tests and checklists to ensure that the development is complying the law.

All personal data which is stored must be documented in what is called a privacy impact assessment (PIA). Along with what personal data is stored, the PIA must also include metadata, like where it is stored, why, and for how long it will be accessible. All processing of data must be included in the PIA along with a description of the scope and purposes of the processing, the necessity and compliance measures. Identifying and mitigating the risks to the consumers is important in the PIA. It will also include information on who can access data and why. Having a PIA is not an option, the document has to be included in all projects since it can be requisitioned by a data protection regulator if there is a concern of privacy or data breach.

We believe that privacy impact assessment is a big change in how developers have to work from now on. One of the developers we talked to had worked a lot on projects that needed to be changed, and said "Privacy by design and PIA seems like a big change of workflow in the start, but will come as second nature, and developers will find these obligations to be common-sense after a while".

We were given advice for current and future developers from one of the developers we were in touch with. One of which is specifically for the coding part in projects, which is to find the right libraries to use. Regarding third party libraries, one should do some research on which of them considers privacy and are compliant with GDPR. The other advice has to do with code reviews. Code reviews should have audits for privacy by design principles to determine where the data is stored (virtually and physically) and how it is secured.

Developers need to have knowledge of what is covered by GDPR and other local or regional laws. The data protection officer is the one responsible for training the employees on a given project, assuring that they have knowledge in the area and are complying with the laws. We expect that the training of new employees in the coming years will be more brief, considering that knowledge of GDPR and other laws will be a prerequisite in job descriptions. Considering GDPR spans over all EU-countries, it will most likely be taught to IT-students. Therefore the companies wouldn't need to use as much resources to educate the employees as they do now. It will still be the

DPOs responsibility to follow up the developers, make sure that they have the knowledge, and are complying.

3.5 Consumers

Although GDPR presents a lot of changes for companies, it's for a good reason. The privacy laws were out of date and companies got away with severe data breaches easily. Much of the focus up until this point has been on businesses preparing for GDPR, but the new regulation is also set to have a sizeable impact on consumers. This is especially in terms of improving how their data is stored and handled, but also their experience as a customer. So what differences might customers notice when the regulation takes effect?

First off, the customers might see a change in the line of communication between them and the business handling their data. Obviously this could differ from company to company, but a good and understandable dialogue with the customer will benefit the business if the competent is aware of their rights. As well as improving the experience of the customer this will also affect the length of various consent statements and policies. That is why it's essential to be unambiguous. It has to be transparent with plain and clear language to make sure it's easily understood by the consumer. The business must obtain consent by "clear affirmative action" when someone signs up for a service.They also cannot be forced to give consent for further use of the data.

Quite a lot of communication with the customer today happens without an explicit thought about its legality. Except for marketing communications, the business of using and storing customers' data to interact with them is just another part of doing the job. Still, when under the GDPR, doing anything regarding personal data or communication will require careful thought. How, for example, will organisations demonstrate that they are processing these data under "legitimate interests"? How will they describe the right to erasure and complex profiling? At this point it is important for the company to be in control of the data being processed and the reasons why, considering the rights of the consumer. When collecting data from children, the need for precision will be even more crucial[24]. Because of this, consumer rights must now be considered by data controllers before undertaking new processing.

The rights of the consumers will have to be taken into account, even though they are not aware of it.

4 Analysis

Based on our research, we wanted to find out how one could improve the process of implementing a law like GDPR or start thinking more about privacy in general in a business. When talking to businesses, we quickly understood that creating attention was a key element in the process of becoming compliant, because every employee isn't up to date with current regulations. Furthermore, the companies we talked to stated that they didn't receive enough support from their local data protection authority, especially with the practical implementation. What some companies did was reading the law in e.g. english or danish, even though there are no guarantee that the norwegian law will state exactly the same because of different juridical practices. A solution to this could also be talking to international law firms that specialize on european law.

The companies we talked to seemed to understand the key changes of GDPR, thanks to own research, seminars and using local law firms to help them out. We would recommend businesses to focus even more on creating attention, establishing a privacy manual, and be consistent about privacy within the whole company.

4.1 Framework

Based on what we learned from this project, we developed a framework consisting of guidelines for how GDPR and privacy initiatives could be implemented in a business.

Activity 1 - Attention and establishment

First off, bringing attention to privacy and GDPR implementation is essential. If a company and its employees are engaged and have knowledge about privacy, the implementation and mapping phase will run smoother.

Action points within this activity:

- The leader group must be active
- Give attention, talk about it, send people to talks and seminars about privacy / GDPR
- Develop a budget and assign a team based on experience with privacy, from different parts of the company

Activity 2 - Overview and mapping

After a team of competent people are gathered, they should perform mapping of the company's usage of personal data. The company needs to find out the different purposes for using the data, where it's being used and stored, and which measures are already in place to ensure users privacy. After mapping has been performed within the company, a gap analysis should be the next step. A gap analysis' main goal is to find out the current status of how privacy is implemented in the company, and then comparing it with how it should be according to GDPR. After a gap analysis is performed, we would recommend booking a meeting with the leader group to show them what needs to be fixed, in addition to a time estimate. In the end of this activity, it could be helpful if the company cooperates with a law firm to make sure every solution in the gap analysis is according to GDPR.

Action points within this activity:

- Mapping processes, types of personal data, categories of personal data (including sensitive), who are responsible for collecting and processing, what systems are being used
- Identification of the need for measures in relation to actual registration and use of personal data
- Perform a gap analysis, and get a clear understanding of what needs to be fixed

Activity 3 - Decisions

After having a clear understanding of what should be fixed to be GDPR compliant, the company needs to make decisions. This could be, but is not limited to, the need of a DPO, where data should be stored and who should be performing the changes needed to be compliant.

Activity 4 - Implementation

After the different decisions has been taken, an implementation project should be started. This means editing processes and privacy practices within the company - based on what the company discovered in the gap analysis. Some key elements that several companies will have to change are what personal data is being processed, how sensitive data is stored, establishing a PIA and implementing privacy by design. This is the most time-consuming and intensive phase of the implementation project.

Action points within this activity:

- Edit processes and privacy practices based on the gap analysis
- Make sure processing of personal data and the use of personal information is being done in compliance with GDPR
- Check that other affiliates of the company are also compliant with GDPR - and make sure they are, by reading their privacy manual, report from a law firm or their PIAs

Activity 5 - Continued attention and development

After the implementation phase is done, the company should be in compliance with GDPR. The company should now focus on how to ensure that it's GDPR compliant also in the future. To do this it needs to be given frequent attention, and both existing and new employees should receive training. It is also important to remember that GDPR is a law that will continue to be improved, but it's important that companies keep up with the edits as well. In addition to this, a privacy manual should be developed in order the make it easier for both existing and new employees to get a better idea of how the

company processes personal information.

Action points within this activity:

- Continue bringing attention to GDPR and privacy
- Provide training for employees
- Construct a privacy manual within the company

5 Conclusion

Although the Data Protection Authority in Norway ("Datatilsynet") has been brief regarding practical information of the GDPR, the businesses we talked to seemed to take the new law and its changes seriously. The law has now been postponed to the 1st of July 2018, yielding them more time to be compliant. For European businesses, the GDPR might introduce a lot of changes, however, for norwegian companies it seems that the changes aren't as drastic, regarding our privacy law already in place. In the end, we believe that the new law will be beneficiary for both consumers and companies by introducing uniform standards throughout the EU, prioritizing individual freedom and giving access to personal data that is stored about us.

6 References

[1] European Data Protection Supervisor. The history of the general data protection regulation. `https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en`.

[2] Council og the European Union. Proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). `http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf`.

[3] W. Scott Blackmer. Gdpr: Getting ready for the new eu general data protection regulation. https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/. published; May 5, 2016.

[4] European Commission. Press release database. http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm. published; Brussels, May 24, 2017.

[5] EDTA. Decision shaping in the european economic area. http://www.efta.int/~/media/Files/Publications/Bulletins/eeadecisionshaping-bulletin.pdf.

[6] Stortinget. Eu/eØs-arbeidet. https://www.stortinget.no/no/Stortinget-og-demokratiet/Arbeidet/EUEOS-arbeid/. Online; accessed May 5, 2018.

[7] Stortinget. Skriftlig spørsmål fra torstein tvedt solberg(a) til justis-, beredskaps- og innvandringsministeren. https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=71294. Online; accessed May 5, 2018.

[8] Kjetil Kolsrud. Gdpr-fristen kan bli utsatt. http://rett24.no/articles/gdpr-fristen-kan-bli-utsatt. published; February 21 2018.

[9] GDPR Article 33. Notification of a personal data breach to the supervisory authority.

[10] GDPR Article 15. Right of access by the data subject. https://gdpr-info.eu/art-15-gdpr/.

[11] GDPR Article 17. Right to erasure ('right to be forgotten'). https://gdpr-info.eu/art-17-gdpr/.

[12] GDPR Article 20. Right to data portability. https://gdpr-info.eu/art-20-gdpr/.

[13] GDPR Article 25. Data protection by design and by default. https://gdpr-info.eu/art-25-gdpr/.

[14] GDPR Article 37. Designation of the data protection officer. https://gdpr-info.eu/art-37-gdpr/.

[15] GDPR Article 83. General conditions for imposing administrative fines. https://gdpr-info.eu/art-83-gdpr/.

[16] GDPR Article 6. Lawfulness of processing. https://gdpr-info.eu/art-6-gdpr/.

[17] GDPR Article 7. Conditions for consent. https://gdpr-info.eu/art-7-gdpr/.

[18] GDPR Article 4. Definitions. https://gdpr-info.eu/art-4-gdpr/.

[19] GDPR Article 30. Records of processing activities. https://gdpr-info.eu/art-30-gdpr/.

[20] Dilligent. The gdpr checklist for directors. https://diligent.com/wp-content/uploads/2017/11/WP0032_US_The-GDPR-Checklist-for-Directors.pdf.

[21] Audun Jøsang. Lecture on information security management. http://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/inf3510-2018-l02-isman-humfact.pdf.

[22] John Chambers & John N. Stewart. Why cybersecurity leadership must start at the top. https://www.forbes.com/sites/frontline/2015/07/13/why-cybersecurity-leadership-must-start-at-the-top/#35a58ce918ab.

[23] Stibbe. Complying with the general data protection regulation (gdpr). https://www.stibbe.com/en/expertise/practiceareas/data-protection/general-data-protection-regulation/how-to-tackle-your-gdpr-compliance-project.

[24] GDPR Article 8. Condition applicable to child's consent in relation to information society services. https://gdpr-info.eu/art-8-gdpr/.

[25] GDPR Article 23. Restrictions. https://gdpr-info.eu/art-23-gdpr/.

[26] GDPR Article 27. Representatives of controllers or processors not established in the union. https://gdpr-info.eu/art-27-gdpr/.

[27] Article 65. GDPR. Dispute resolution by the board. https://gdpr-info.eu/art-65-gdpr/.

[28] Heather Burns. How gdpr will change the way you develop. https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/.

[29] Information Commissioner's Office. Data protection impact assessments. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

[30] Bryan Soltis. I'm a developer and gdpr is no big deal. or is it? https://hackernoon.com/im-a-developer-and-general-data-protection-regulation-gdpr-is-no-big-deal-or-

[31] Rosemary Smith. Will the gdpr really make a difference to consumers? https://www.dpnetwork.org.uk/opinion/will-the-gdpr-really-make-a-difference-to-consumers/.

[32] Nick Ismail. How will gdpr impove the customer experience for consumers? http://www.information-age.com/will-gdpr-improve-customer-experience-consumers-123470312/.

[33] Glen Kunene. The gdpr: What it means for customer communication. https://www.nexmo.com/blog/2017/11/14/gdpr-means-customer-communications/.