General Data Protection Regulations

Guidelines for Developers and Designers

Mehrnaz Ataei,Sofian Slimani,Christian Kray

GDPR for developers and designers

January 24, 2020

Executive Summary

Key Results and Findings

1. **GDPR requirements should be adjusted and designed for particular needs.** Complying with data protection regulations can become challenging for those who are responsible for the final implementation of the privacy protection measure; therefore, there is a need to adjust the presentation of the regulation to the specific needs of various user groups.
2. **GDPR should be formulated for developers and designers.** GDPR requirements should be provided to designers and developers in a way that is relevant to the software development life cycle, one approach would be the integration of legal requirements into the software development life cycles.
3. **Development of an interactive platform for developers and designers.** This project developed an interactive tool for presenting GDPR related information to those responsible for its implementation. The interactive tool connects the GDPR requirements to the software development life cycle (SDLC) to help developers teams in their GDPR compliance journey.

The General Data Protection Regulation (GDPR) is meant to protect users privacy by establishing a series of obligations for service and system providers. Eventually, developers and designers are the main groups who are responsible for taking practical actions towards compliance with GDPR, but one of the main problems is that GDPR does not provide explicit guidelines for designers and developers about how to build GDPR compliant products. In order to bridge this gap, we systematically analysed the GDPR text and carried out a user study to understand the current challenges regarding the GDPR compliance, then we designed a platform that connects the content of GDPR to the software development phases, such presentation of content provides relevant information for developers and designers in every stage of the development process, the platforms also include relevant external links for further information.

Contents

1 Introduction

Majority of the software, services and tools developed for human users regularly collect users' personal data. The rationale behind such behaviour is often justified as providing users with relevant and customised information. While on the surface, this argument is reasonable, there are a couple of fundamental issues with the collection of personal data on regular bases. Personal data is sensitive because it has the potential to reveal information about individuals and also it can infer a deep level of knowledge about people. Unwanted disclosure of such private information can lead to the violation of privacy can have negative influences on individuals lives [1]. Privacy violations can also lead to concerns regarding massive surveillance in societies [3]. Thus, it is crucial to develop means to protect privacy in order to maintain values like freedom and basic rights for humans in societies.

A number of solutions and measures have been developed to protect data. For instance, technical measures have been designed to keep the data as secure as possible, or legal safeguards which establish standards and principles to protect individuals rights through legal means. The General Data Protection Regulation (GDPR) [2] is one of the recently updated and improved legal safeguards which introduced by the European European Union (EU) to reinforce the protection of personal data in Europe.

GDPR came to effect on May 25th 2018, to protect the privacy of the EU citizens. GDPR sets a number of legal requirements for those who are involved in activities such as collection, storage, use and process of personal data. GDPR's legal expectations have impacts on the current practices of developing services and software. There has been an ongoing debate and efforts from various stakeholders to find best practices to comply with new sets of regulations.

There are a number of steps to take before deciding which type of tools or services one should use to become GDPR compliant. The first step is to determine whether the company must comply with the regulation. If a company collects, stores or processes personal data* of the EU citizens, that company must abide by the rules. The second step is to determine the role of the company as a controller*, processor* or both. Clarifying the position is crucial as GDPR has established different responsibilities for different roles. The further steps depend on various factors such as companies size or their specific businesses but in the majority of the cases, the combination of different solutions is needed for becoming GDPR compliant.

Through this research project we aimed at addressing challenges that the introduction of GDPR has caused for software development teams and companies by 1)systematically analysing and compiling the GDPR document to extract essential factors relevant to software development life cycle; 2)carrying surveys to gather insights about the most challenging factors in companies; and by 3) developing a guideline which integrates essential factors in GDPR to SDLC stages to facilitate the compliance journey by developers and designers. Our contributions can benefit, software providers and development teams who should consider GDPR requirements in the process of developing services, tools and software.

The following sections of this report summarise existing solutions and tools developed to assist the GDPR compliance in section . Then introduces the concept and design development processes in section 3, it then presents the result of a survey regarding the current stage of companies GDPR implementations and also the challenges and difficulties that developer teams encounter on their way to become GDPR compliant in section 4. It continues by section 5, which is about the analysis of the GDPR document and the list of essential topics relevant to software development processes. Section 6 presents tasks in SDLC phases with respect to GDPR requirements and external links to more detailed instructions. This report eventually discusses and proposes an online platform developed as a tool to facilitate the integration of legal requirements into the software development life cycles (SDLCs) in section 7 and finalise the results by a discussion in section 8.

2 Existing Solutions for Developers and Designers

There are different parties producing guidelines, frameworks, and tools to facilitate compliance. We have categorised these frameworks into three groups; (1) Official document and guidelines developed by EU commission or data protection authorities in each state, (2) Educational sources, including guidelines to facilitate the understanding of the GDPR official document developed by various parties such as companies, legal firms or educational entities. and (3)data privacy management tools that are software developed by tech vendors to facilitate compliance with GDPR through digital means. The following is the list of the resources from groups mentioned above. The final section of the list covers the resources developed in German language.

2.1 Official Sources

1. Plain GDPR [1]document in different languages, is the primary official source for the General data protection regulation. The aim is to protect individuals (i.e. natural persons) with regards to the process of their personal data. The document includes 173 Recitals and 99 articles.

2. Official EU website [2] provides the GDPR document. It also presents additional relevant information like GDPR background and related policies. It also highlights essential questions such as what is personal data? Or what does the GDPR govern?

3. European data protection board (edpb) [3] is an official source that provides general guides, recommendations and best practices regarding the GDPR. edpb provides insights on individuals right, controllers processors, and regulators. The guidelines have developed based on different aspects of GDPR such as transparency, consent, and data subjects' rights.

4. The content of this website [4] includes official GDPR document therefore listed in this section, otherwise it is not an official source, GDPR document which is presented in an accessible manner in both English and German. The site has organised all the articles and recitals in a way that it also shows the articles links to each other and corresponding Recitals. Searching and finding specific information is much easier in comparison with the plain GDPR document.

2.2 Data Protection Supervisory Authorities

1. Data protection authorities [5] are responsible supervisory authorities for data protection in each state. Individuals or organisations should contact them for questions regarding data protection laws. Data protection supervisory authorities in each member state are listed here.

2. In the case of Germany, according to edpb Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [6] acts as a supervisory authority. However, there are a number of supervisory authorities in different areas according to this list.

   While each member state follows a similar approach regarding GDPR's implementation and provide support for organisations, companies, and individuals. Some are providing more detailed guidelines and assessment tools to facilitate compliance for different stakeholders. Two following examples are from France and the UK:

3. Data protection authority website in France has provided a data privacy impact assessment (DPIA) tool[7].

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298uri=CELEX:32016R0679

[2] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules$_en$

[3] https://edpb.europa.eu

[4] https://gdpr-info.eu

[5] https://edpb.europa.eu/about-edpb/board/members$_en$

[6] www.bfdi.bund.de/

[7] https://www.cnil.fr/en/guidelines-dpia

4. Information commissioner's office (ICO) in UK has provided a guide to data protection [8] together with a data protection self assessment [9].

2.2.1 Educational Sources and Guidelines

1. GDPR portal [10] provides an overview of the GDPR and also presents changes from data protection directive to GDPR.
2. A comprehensive guideline [11] developed by the UK's information commissioner's office (ICO).
3. Teach privacy [12] provides guidelines, articles and insights about data protection in general including GDPR specifically. This website is an educational source for data protection and relevant topics.
4. Privacy Index [13] is a curated index of GDPR resources including companies, products and services for GDPR compliance. It also outlines 12 steps suggested by ICO to prepare for GDPR.
5. White case website [14] provides an excellent overview on articles and recitals of GDPR and also compares the changes with the directive and summarises the impact from a legal perspective.
6. This guideline [15] aims at explaining GDPR for marketers and businesses.
7. This guidelines [16] is similar to the previous guide, with some example aiming at GDPR for marketing.
8. Data protection network website [17] provides insights and opinions on GDPR.
9. An understandable GDPR guideline [18] developed by Two Birds law firm provides an easy to follow guide for GDPR compliance.
10. The International Association of Privacy Professionals (iaap) [19] is a partially free educational source for various data privacy-related material including GDPR.
11. Official EU website [20] provides infographics to summarises data protection rules.
12. IMB [21] also provides a short introduction for GDPR.
13. Data Guidance [22] provides privacy solutions by monitoring regulatory developments, GDPR portal and in depth guidance by experts.
14. Munich Re [23] provides a Web tool to guide staff about data protection. It monitors the data workflow and provides guidance based on that.

[8] https://ico.org.uk/for-organisations/guide-to-data-protection/

[9] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

[10] https://eugdpr.org

[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

[12] https://teachprivacy.com

[13] https://gdprindex.com

[14] https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protectiontoc

[15] https://appinstitute.com/gdpr-guide/

[16] https://www.superoffice.com/blog/gdpr-marketing/

[17] https://www.dpnetwork.org.uk

[18] https://www.twobirds.com/ /media/pdfs/gdpr-pdfs/bird–bird–guide-to-the-general-data-protection-regulation.pdf?la=en

[19] https://iapp.org/

[20] https://ec.europa.eu/justice/smedataprotect/index$_{e}n.htm$

[21] a short introduction for GDPR

[22] https://www.dataguidance.com

[23] https://www.munichre.com/complianceweb/en

2.3 Privacy Impact Assessment (PIA) Guides

1. ICO provides [24] for businesses including checklists for controllers and processors.
2. ICO also provides DPIA templates [25].
3. eprivacy website [26] provides an overview of PIA.
4. Overview and a summary of PIA can be found here [27].
5. IBM provides GDPR self assessment for businesses [28].

2.4 Privacy Management Software

Beside official sources and general guidelines, many privacy vendors and tech companies have developed or developing privacy management tools with the aim of automating the compliance process. These tools provide various services on different levels. From mapping the data to producing audit reports. International Association of Privacy Professionals (iapp) [29] has listed the name of companies producing privacy management software and tools [30], including assessment managers, consent managers, data mapping, privacy information managers and, etc. The report contains over one hundred companies and a summary description of their products. The following lists are the companies that are the most relevant for GDPR compliance as they provide the combination of at least three different services. In order to be able to compare their services, we used the list of services presented in the iaap report and categorised them into two groups. Inspection group that includes Activity Monitoring, Assessment Manager, Data Discovery, Data Mapping and Website Scanning. Action group that includes Consent Manager, Incident Response, Privacy Information Manager, De-identification/Pseudonymity. The list shows only the companies that provide no less than three services with at least one service from each group (See Appendix A for the list of the companies)

2.5 Existing Solutions in German Language

Organisation of GDPR supervisory authorities in Germany
As a federal country, Germany holds individual GDPR supervisory authorities for each state as well as a nation-wide authority. State level data protection authorities are responsible for companies, other non-public organizations and state- or municipality-level public authorities inside their boundaries.

Exceptions to this exists for companies in the area of telecommunication and postal services where the nation-wide authority is responsible [31]. Further, the nation-wide data protection authority is responsible for all other nation-wide authorities and certain social security institutions, e.g. statutory health insurance companies [32]. For communication and coordination between the different data protection authorities a committee (called DSK) exists. Part of this committee is the 'Düsseldorfer Kreis', coordinating the authorities responsible for non-public organizations. Regardless of this, differences in the enforcement of GDPR exists between the different state-level data protection authorities, e.g. in the extent of controls and fines [33].

GDPR Guidance material provided by German public authorities
The DSK committee provides several short papers regarding some major topics of GDPR [34], including an action plan for companies [35]. However, this plan does not provide detailed guidance but gives a broad overview of steps

[24] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

[25] https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

[26] https://www.eprivacy.eu/en/consulting/data-privacy-impact-assessment/

[27] https://blog.lukaszolejnik.com/data-protection-impact-assessment-first-guidelines/

[28] https://www.ibm.com/data-responsibility/gdpr/

[29] https://iapp.org

[30] https://iapp.org/media/pdf/resource$_{c}enter/2018 - Privacy - Tech - Vendor - Report.pdf$

[31] https://www.bfdi.bund.de/DE/Infothek/Anschriften$_{L}inks/AnschriftenUndLink.html$

[32] https://www.bfdi.bund.de/DE/BfDI/Artikel$_{B}FDI/AufgabenBFDI.html$

[33] https://doi.org/10.1007/s11623-015-0521-6

[34] https:// www.datenschutzkonferenz-online.de/kurzpapiere.html

[35] https://www.datenschutzkonferenz-online.de/media/kp/ dsk$_{k}pnr8.pdf$

companies have to take to comply with GDPR. Additionally, the DSK provides detailed guidance for four fields of use [36]: Company-intern whistleblowing hotlines, Direct Marketing, Online-learning platforms in schools and information collection of prospective tenants.

The 'Düsseldorfer Kreis' provides guidance material for privacy law compliance through the websites of the state- and nation-wide data protection authorities. The guidance material provides information for different target groups, e.g. 'Requirements to app-developer an app-provider' [37], [38]. However, this material (as of 06.02.2019) is outdated and does not consider the GDPR.

The Federal Ministry of Economic affairs and Energy provides a checklist for GDPR compliance in companies [39]. The state-level data protection authorities provide a similar checklist [40]. However, similar to the DSK short paper, these checklists do not provide detailed information for certain use-cases but rather give broad suggestions to which aspects companies should pay attention.

difficult The organisation of data protection authorities as well as the provision of outdated guidance makes it difficult to find official information for GDPR compliance among German public authorities. Detailed and easy-to-understand information for technical purposes is not given. Due to partially spread panic among individual developers and small companies and the lack of public guidance before the GDPR came in to power, (partly dubious) commercial guidance offers arised. Since the GDPR came into power this panic decreased enormously.

Besides the mentioned sources, there are more GDPR guidelines and solutions, developed for German users, for instance:

1. The Industrie- und Handelskammer (IHK) München [41] provides useful information about GDPR compliance, including a simply written sample case of a small service company and a 10 steps overview plan.
2. The Bayrisches Landesamt für Datenschutzaufsicht (LDA) (official supervisory authority) provides a checklist for GDPR Compliance
3. The Wirtschaftskammer Österreich (Austrian Economic Chamber) provides various GDPR guidance, including information and Checklist for Cookies and Web Analysis in Web Shops
4. There are various commercial GDPR plugins aiming at simplifying the actual process of reaching GDPR compliance with a website or an online shop. One example for this is 'WP DSGVO Tools [42], a plugin for Word Press.

3 Concept Development

Understanding developers and designers current difficulties in their GDPR compliance journeys is the first step towards developing guidelines and solutions for them. Thus, a survey study was conducted to gather initial insights about challenges that developers and designers of IAI members encounter regarding the implementation of the GDPR. The result of this study is presented in section 4 While the intention and rationale of updating data privacy protection regulations by EU commission in a harmonised way are all positive and necessary, it is not reasonable to expect involved parties to comply with the rules without encountering challenges and difficulties. In compare to the previous version of the regulation (i.e. Directive 95/46/EC), a number of relevant concepts to today's technical advancements have been presented in the GDPR. One of these concepts, emphasises on the following the Privacy by Design principles, which means integrating privacy protection measures into the development process of developing digital services instead of considering privacy-related issues after building software or services. The development teams are usually responsible entities to fulfil such requirements. The challenging aspects are related

[36] https:// www.datenschutzkonferenz-online.de/orientierungshilfen.html

[37] https://www.lda.bayern.de/en/guidelines.html

[38] https://www.bfdi.bund.de/DE/Infothek/ Orientierungshilfen/orientierungshilfen-node.html

[39] https://www.bmwi.de/ Redaktion/DE/Publikationen/Digitale-Welt/datenschutzgrundverordnung.pdf? $_{blob=publicationFilev=16}$

[40] www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/05/10-Punkte- Papier$_PM_Datenschutz-bleibt-Chefsache.pdf$

[41] https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Die-EU-Datenschutz-Grundverordnung/

[42] https://de.wordpress.org/plugins/shapepress- dsgvo/

to translating legal requirements to practical tasks which can be implemented during the software development processes.

As mentioned in section 2, several resources are aiming at facilitating the compliance process by developing, guidelines, frameworks and tools. These sources include guidelines developed by EU commission as supplementary materials to the original GDPR document. Each EU state has one or more data protection authorities which are also producing and developing guidelines about data protection regulations. Besides information and guidelines, there are several tools designed to automatise the process of complying with GDPR in companies dealing with GDPR.

Despite all the produced material and developed software, it is still difficult to find a free source which includes necessary information for understanding the GDPR's requirements and also provides the possibility of having access to the details of regulation at the same time. In order to have access to all essential requirements, one should use a different group of sources at once, for instance, a summary of important factors to address together with the original document and also a list of practical instructions.

We aimed at addressing the problem of making GDPR accessible for developers and designer through providing an accesses through different levels of information, i.e. an overview of an important topics from GDPR, their connection to SDLC phases and also on a deeper level, articles and recitals and even a simplified version (i.e. plain English) of the latter. The following sections (i.e. section 6) present the analysis processes of legal text and the list of relevant topics with a short description about them. The next stage was related to SDLC phases and their connections to the important matters established by GDPR, relevant topics were then assigned to one or more of the SDLC phases to support the connection that development process requires in order to integrate privacy related matters to software development process.

Selecting important topics from GDPR and connecting them to SDLC stages were the steps we took to build the foundation for an interactive tool for developers and designers. To realise how this information can be shown in different levels from general overview to detailed articles and recitals, we designed a platform wich has been presented in section 7.3.

4 Study Design

The goal of this study was to build guidelines for developers and designers to facilitate the process of complying with the General data protection regulation (GDPR), particularly during the software development processes. Therefore, it was crucial, to begin with understanding the challenging aspects of GDPR requirements in order to develop a solution suitable for developers and designers needs.

A survey including questions about the main requirements of GDPR was designed to identify the most challenging aspects of compliance with GDPR for developers team and privacy professionals in companies. After the approval of the Institute For Geo- Informatics ethic board, both German and English versions of the surveys were mailed to around 30 companies (i.e. IAI members). We requested that the servery be filled by those who are responsible or involved in the process of implementing GDPR requirements in the company, 17 individuals with different occupations including developers, managers, directors, Data protection officers, compliance officers, and assistance for GDPR were responded to the surveys.

4.1 Study Result

The survey design aimed at covering aspects of GDPR requirements relevant to software development processes. The survey started with a few questions regarding the participants' occupation, their companies current situation regarding the implementation of the GDPR requirements as well as their method of managing GDPR in their companies.

Regarding the current stage of the companies' compliance with GDPR requirements, two have not implemented or planned any activities yet. Eight have partially implemented all the GDPR requirements, and seven have successfully implemented all the GDPR requirements.

Nine companies manage tasks regarding GDPR compliance manually, three out of these nine combine the manual means with other tools such as commercial software. One of the companies used the combination of commercial software and an external consultancy firm to manage GDPR related tasks. Only one of the companies has developed software internally to manage GDPR related tasks.

Participants selected the level of easiness difficulties for 18 subjects which covered essential aspects of data protection requirements. The questions include the essential principles that a company, dealing with the collection and process of personal data, must consider for becoming GDPR compliant (See Appendix Bfor the survey question and Appendix C for survey result).

The survey presented 18 statements covering various GDPR topics and participants were required to rate the level of difficulties of each of these tasks in the form of statements with four options including 1)easy 2)moderately easy, 3)moderately difficult and, 4) difficult.

Understanding of the GDPR requirements (Q6) was rated as moderately easy for 47.1% and moderately difficult for the same amount. While 5.9% found it difficult, no one rated it easy.

Q6.I find the understanding of GDPR requirements ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
0.0%	47.1%	47.1%	5.9%	0.0%

Finding guidelines, instructions, tools or proper resources for becoming GDPR compliant was perceived difficult by 5.9%, moderately difficult by 47.1% of the participants while 29.4% found it moderately easy and 11.8% found it easy.

Q7. I think finding guidelines, instructions, tools or proper resources for becoming GDPR compliant is ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
11.8%	29.4%	47.1%	5.9%	5.9%

The level of difficulty about mapping out the data flow rated as moderately difficult for 41.2% and difficult for 5.9% of the participants, while 17.6% found it easy and 35.3% found it moderately easy.

Q8.I think mapping out the data flow in our company is ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
17.6%	35.3%	41.2%	5.9%	0.0%

A few statements also covered tasks regarding the management of the data and providing means for data subjects. Two of the statements had the highest level of difficulty, documenting the information about the collected personal data (Q10) such as its source or the period that the data is going to be kept rated moderately difficult by 52.9% and difficult by 29.4% of the participants. The same level of difficulty was expressed for the task of providing users with their personal data collected about them.

Q10.I find documenting the information about the collected personal data such as its source or the period that the data is going to be kept ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
0.0%	17.6%	52.9%	29.4%	0.0%

The management of consent forms which is one of the GDPR's important aspect was rated as easy by 5.9%, moderately easy by 29.4%, moderately difficult by 41.2%, and difficult by 17.6% 5.9 of the participants.

Q15.I find Managing consent forms ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
5.9%	29.4%	41.2%	17.6%	5.9%

It was interesting and expected to see that while securing collected data was perceived as moderately easy by 64.7% of the participants; this number dropped to 29.4% when the statement was about the security of the transferred data.

Supporting transparency as one of the GDPR's main concerns seems manageable by participants as they have found the communication of data management with end users easy (29.4%) and moderately easy (47.1%). While the communication of what's happening to users about the collected data seems feasible, providing users with the collected data about them is a bit more challenging as it has been rated moderately difficult and difficult by 52.9% and 29.4% by participants. Performing data protection impact assessment (DPIA) rated as one of the most challenging factors by 70.6% moderately difficult and 5.9% difficult. Another challenging task is to keep track of all the tasks and documentation in the compliance process.

Figure 4.1 presents an overview of the result with all the statements and the responses. The overview points out the answers of the participants to the statements from question No.6 to question No.23 (see Appendix B for the statements).

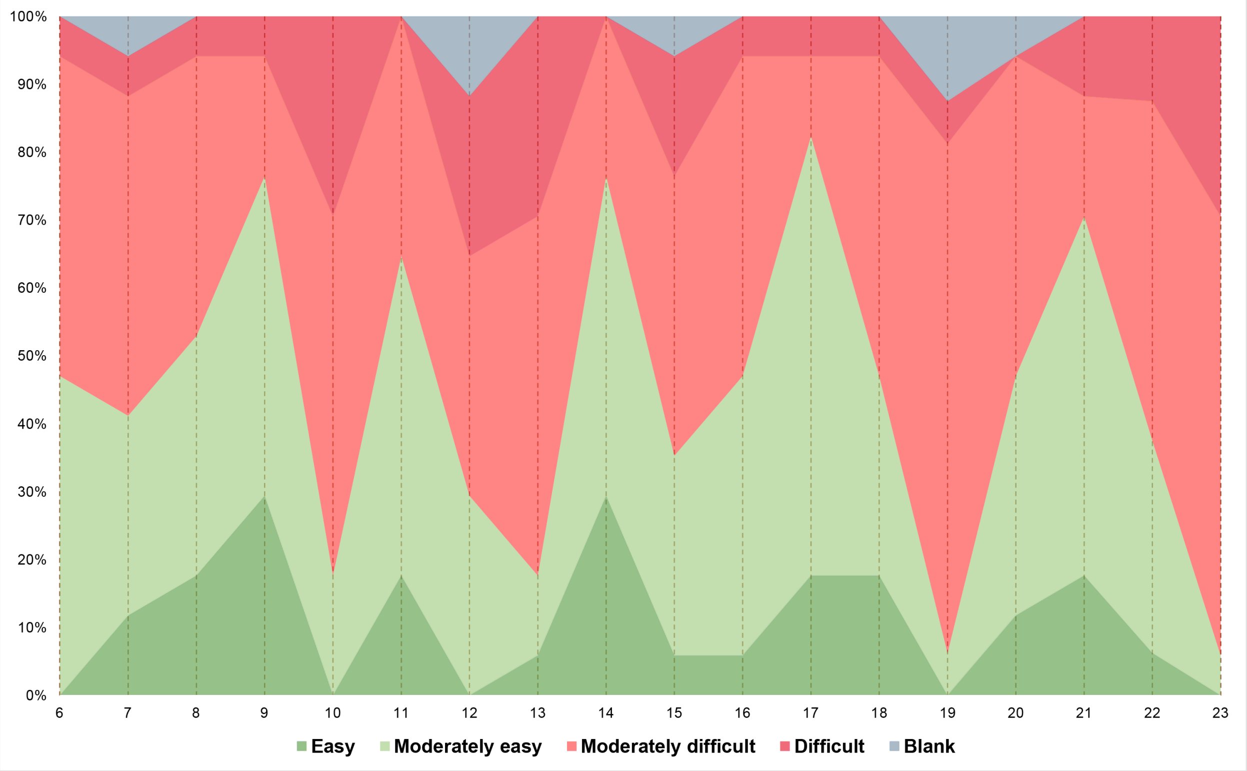


Figure 1: Overview

In addition to the Likert scale questions, the final part of the survey required participants to mention challenging matters which were not mentioned in the questionnaire.

P3, P5 and P13 mentioned the tasks of going through the data sets in order to delete the unwanted data, keeping track of deleted sets and also securing the data as a few challenging tasks. P3 also pointed at that anonymising large databases is demanding.

Understanding the level of the risks associated with data management decisions were what P8 mentioned as one of the challenges: "To understand which risks are allowed to tolerate to not restrict the entrepreneurial freedom too much". P8 also thinks that the understanding of the practical implementation is missing in existing material and practices.

P10 indicated that the assessment of communicating incidents with data protection authorities as a challenging task: "To assess when a Data protection event has to be reported to the supervisory authority'. P10 also thinks that the

"GDPR is a 'step in the right direction', but at many points very 'bulky'".

P15 mentioned that right now there are facing two sets of rules, the challenge is to decide about which one to follow?! "GDPR, BDSG (German data protection law), Landesdatenschutzgesetz (data protection law of each German state) [...] Which applies now?"- P15.

P14 found the Installation of Awareness program challenging, p4's personal view on GDPR implementation is that the: "In view of globalisation it is hard to believe it will change anything to the good" - P14.

P16 lists the challenging factors for them as; 1) "Data processing agreement with supplier including sub companies", 2) create individual data protection for various stakeholders including third-parties, 3) Privacy conform handling of Job Candidates and, 4) technical realisation of consent-management (Opt-In/Opt-Out), and 5)Keep track of processing activity.

The result of the survey points in many aspects that individuals responsible for the implementation of GDPR in companies are finding difficult. After clustering these challenges to GDPR requirements' understanding, management, communication and activity tracking. We decided to focus on two aspects, Information finding and keeping track of the activities which has direct effects on DPIA and audits.

5 Legal Document Analysis

After compiling the list of challenges as the result of the survey,an iterative design process was conducted to analyse the GDPR document and extract relevant key topics to the development process of information systems. The list of the key topics with their description is presented in the this section. These key topics provide a general view of essential definitions and requirements in GDPR that are relevant to everyone who aims at implementing GDPR requirements during their software development processes. A group of key topics had been defined to include important concepts that are crucial to be discussed during each software development phase (presented in section 6). These topics provide an overview of an important subject, but they also connect to one or more of the software development phases in order to link relevant information to the activities in each stage of developing software. A brief explanation of each these phases with regard to data protection activities are presented in 6.

5.1 Key Topics

5.1.1 Personal Data

It is crucial to understand the definition of personal data, as GDPR applies to this type of data. According to Art.4(1) GDPR, "personal data means any information relating to an identified or identifiable natural person ('data subject')". The personal data considers as sensitive data when it reveals race or origin of individuals which if processed, might cause risks to the fundamental rights and freedom - Rec.51 GDPR. The processing of personal data should be lawful, which means the processing should follow fair practices such as data protection principles and data subjects rights. There are two important definitions for data sets in this context: [43]

Art.4(1), Art.6, Art.25, Art.32(1)(a) Rec:(26),(28),(29),(78),(34),(35),(30),(51)

- Anonymous data: GDPR does not apply to Anonymous data ONLY if there is no way that individuals can be identified through such anonymous data sets.

  Art.6(4)(e), Art.25(1), Art.32(1)(a) Rec:(26)

- Pseudonymous data: pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information Art.4(5).Pseudonymised data is categorised under personal data as there is the possibility of identifying individuals through pseudonymisation, but if the security measures are assured, Pseudonymous data associated with lower risk and therefore requires a lower level of protection.

  Art.4(5), Art.6(4)(e), Art.25(1), Art.32(1)(a) Rec:(26),(28),(29),(78)

[43] https://www.whitecase.com/publications/article/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation

External Links:

- European Data Protection Supervisors → link
- Intersoft consulting → link
- Key Definitions from White Case LLP → link

5.1.2 Data subjects' rights

A number of rights are provided for data subjects(i.e. an identifiable natural person) by GDPR to ensure fair and lawful processing of the personal data. Data controllers are responsible for providing data subjects with means to practise their rights.[44] Such means should be discussed and realised during the development processes.

Art.5, Art.12, Art.13, Art.14, Art15, Art.16, Art.17, Art.19, Art.20, Art.21 Rec:(39),(58),(59,)(60),(61)

- Transparency: All activities regarding personal data such as collecting or processing, must be appropriately communicated with data subjects. The principle of transparency requires that any information addressed to the public or the data subject be concise, easily accessible and easy to understand. The information should be presented in a clear and understandable language and, additionally, where appropriate, visualisation should be used.

  Art. 5(1) Art.12. Art.13. Art.14 Rec:(39),(58),(59,)(60), (61),(65),(66),(67),(68),(69),(70)

- Be informed about the data collection, processing activities and other relevant information: To follow the principles of transparency, data subjects should receive appropriate notice regarding the collection and process of their personal data[45].
  Art.13. Art.14 Art.19 Rec: (60),(61)

- Right of access: Data subjects should be able to have access to the data collected about them. [46] Art.15 Rec:(63),(64)

- Right to rectification: Data subjects should be able to correct their personal data in the case of error.

  Art.5(1)(d), Art.16 Rec:(39),(65)

- Right to erasure ('right to be forgotten'): Data subjects should be able to ask for the deletion of their personal data.[47]

  Art. 17 Rec:(65),(66)

- Right to restrict processing: Data subjects should be able to limit or stop the process of their personal data.
  Art. 18 Rec:(67)

- Right to data portability: Data subjects should be able to transfer their personal data to a different controller.
  R Art. 20 Rec:(68)

- Right to object processing for various reasons: Based on the reasons for processing personal data, data subjects should be able to pause or stop the process of their personal data.

  R Art. 21 Rec:(69),(70)

External link:

- European commission→ link
- ICO - Data Protection Authority UK→ link
- Rights of Data subjects from White Case LLP→ link

[44] https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation

[45] https://gdpr-info.eu/issues/right-to-be-informed/

[46] https://gdpr-info.eu/issues/right-of-access/

[47] https://gdpr-info.eu/issues/right-to-be-forgotten/

5.1.3 Consent

Consent is one of the main and known bases for the lawful processing of data. A number of characteristics have been defined for a consent that can be considered as legally valid. Consent should be freely given, so the data subjects must have been provided with means for voluntary choices and the possibility to reject. Data subjects should also be appropriately informed about the nature of processing with understandable language; data subjects should also be informed about the identity of the controller and processing purposes.[48] Realising all these attributes and designing and managing consent forms should be addressed during the development processes.

Art.4(11), Art.6, Art.7, Art.8 Rec:(32),(33),(38),(59),(40),(42),(43),(50),(171)

External links:

- European commission→ link
- ICO - Data Protection Authority UK→ link
- Intersoft consulting→ link

5.1.4 Data management

Management of the personal data, including the purpose of processing, data collection and data minimisation requires careful decision making according to GDPR.

Art.4(12, Art.5, Art. 6, Art.32, Art.33 ,Art.34

Rec: (39),(40),(41),(44),(45),(46),(47),(48),(49),(50),(83),(85),(86),(87),(88)

- lawful basis for processing: The processing of personal data must be lawful. Processing is lawful under specific conditions such as data subject's consent, contracts that make the processing of the data necessary, legal obligations by controllers to ensure compliance, vital interests of data subjects, public interests where processing is necessary for public authorities, or legitimate interests of controller. The list of these conditions are summarised here.[49]

  Art. 6 Rec:(40),(41),(44),(45),(46),(47),(48),(49),(50)

- Data collection principles: Data collection and processing must be limited to only the personal data that is absolutely needed for specific purposes. It is crucial that the purpose of data processing is communicated with data subjects; also, if the data is collected for one purpose, it can not be processed for other purposes. Further, data controllers must ensure that the collected personal data is accurate. Data retention period and for how long the collected data is going to be kept is also essential according to data protection principles and needs to be defined in the early stages of the development process.

  Art.5(1)(b), Art.5(1)(c), Art.5(1)(d), Art.5(1)(e) Rec:(39)

- Data security: Collected data must be kept secure through various security measures, and controllers are responsible for ensuring such security measures.

  Art.5(1)(f), Art.32 Rec:(39),(83)

- Data breaches (incident management): Incidents must be managed and reported in a proper, informative, and time-limited manner.

  Art.4(12), Art.33, Art.34 Rec:(85),(86),(87),(88)

External links:

- Data protection principles from from White &Case LLP→ link
- ICO - Data Protection Authority UK→ link

[48] https://www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation

[49] https://www.whitecase.com/publications/article/chapter-7-lawful-basis-processing-unlocking-eu-general-data-protection

5.1.5 Processing

Activities related to the collection, process or any other operation on personal data can be considered as processing and entities involved in such activities are required to comply with the regulations. GDPR has defined responsibilities regarding the data processing activities and has also categorised the possible involved parties into two primary groups of controllers and processors. A number of tasks are set for both processors and controllers; it is essential for the software development team to identify their companies' role regarding the processing of the data (i.e. to clarify the role of the company as processors, controllers or both).

Art.4(2), Art.4(7), Art.5(2), Art.24, Art.26, Art.27, Art.28, Art.30

Rec:(26),(74),(75),(76),(77),(79),(80),(81),(82),(83),(85),(87),(88),(97),(101),(102)

- Data Controller responsibilities: The controller defines the purpose of data processing and therefore is responsible for ensuring compliance with the regulation. [50]

  Art.4(7), Art.5(2), Art.24, Art.26, Art.27, Art.28, Art.30 Rec:(74),(75),(76),(77),(79),(80),(81),(82)

- Data Processors responsibilities: The processor has the responsibility of processing the personal data on behalf of the Controller. The processor is responsible for ensuring the confidentiality of the personal data that is going to be processed.[51]

  Art.4(8), Art.28, Art.29, Art.30, Art.31, Art.32, Art.33(2), Art.37, Art. 44

  Rec:(81),(82),(83),(85),(87),(88),(97),(101),(102)

External links:

- EU commission→ link
- Processing from Intersoft consulting→ link
- ICO - Data Protection Authority UK→ link

5.1.6 Privacy by Design

Privacy by Design (PbD) has been initially developed by Cavoukian [52] emphasises on "prevent privacy invasive events before they happen", therefore it supports the idea of integrating privacy protection measures into the software development processes. While GDPR presents a general description of Privacy by Design. The initial idea consists of seven principles:

1. proactive not reactive: rather than wait for privacy risks to occur, such risks should be anticipated and prevented from materialising.
2. privacy as the default setting: the default behaviour of a system should be such that the privacy of its users is automatically protected - no prior user action is required.
3. privacy embedded into Design: rather than 'patching' a system with some privacy-protection measures, privacy-related functionality should be considered as an integral part of the system and be realised without interfering with its overall purpose.
4. full functionality: unnecessary trade-offs (e.g. security vs. privacy) should be avoided, and all legitimate requirements should be realised ("win-win").
5. end-to-end security: all data collected in the system should be protected by strong security at all stages of its life cycle (from creation to deletion).

[50] https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection

[51] https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection

[52] https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

6. visibility and transparency: all parties involved in the provision of a service and the running of the corresponding system, should expose their practices, policies and technologies so that they can be independently verified.
7. respect for user privacy: the interests, needs, and preferences of users should be considered first and foremost to ensure a user-friendly privacy-preserving system.

Art.25 Rec:(78)

External links:

- Privacy by Design from Intersoft consulting→ link
- ICO - Data Protection Authority UK→ link

5.1.7 Data Transfer

Transferring personal data can only happen if specific conditions are met. A number of conditions are listed in GDPR,but one of the bases for data transfer can be the confirmation from data subjects, which should be collected in the form of consent. One of the essential aspects of data transfer is to ensure the security of the data while transferring. This must be realised by data engineers, developers and parties responsible for data securities.

Art.44 Rec:(101) (102)

External links:

- EU commission→ link
- Intersoft consulting→ link
- ICO - Data Protection Authority UK→ link
- Cross border data transfer from White Case LLP→ link

5.1.8 Consequences of Non-Compliance

Data Protection Authorities can issue fines up to 20M euro or 4% of companies annual revenue. Data protection authorities are responsible for assessing and issuing such fines. While a financial loss is an important factor for companies, and compliance with the regulation is necessary to avoid such fines, it is also important for the developers and designers to receive information regarding the negative impacts that the loss of privacy can have on individuals lives.

Art.83 Rec:(148),(150),(151)

External Links:

- EU commission guideline→ link
- EU commission guideline→ link
- Intersoft consulting→ link
- ICO - Data Protection Authority UK→ link
- Remedies-and-Sanctions from White Case LLP→ link

5.1.9 Data Protection officer (DPO)

Data Privacy Officer is the main contact person assigned in companies who is dealing with the collection or the process of personal data to assure the GDPR compliance. DPO's presence during the development process is crucial for ensuring compliance.

The responsibilities of DPO are listed here [53] by European commission:

- inform Commission departments collecting personal data ('controllers') and persons whose data are collected ('data subjects') of their rights and obligations under Regulation 45/2001.
- ensure Commission departments comply with the law when processing personal data investigate data-protection matters.
- keep a register of processing operations on personal data by commission departments cooperate with the European Data Protection Supervisor. [54]

Art.37, Art.38, Art.39, Rec:(97)

External links:

- EU commission guideline→ link
- ICO - Data Protection Authority UK→ link
- DPOs from White Case LLP→ link

5.1.10 Data Privacy Impact Assessment

Data protection impact assessment (DPIA) includes assessment of the data collection and its processing in order to 1)measure and determine the possible risks associated with such activities and 2)the possibility of demonstrating that the appropriate means were used to mitigate potential risk and eventually confirm the compliance with GDPR. European commission's report [55] refers to DPIA as "a process for building and demonstrating compliance".

"A DPIA is required whenever the processing is likely to result in a high risk to the rights and freedoms of individuals". DPIA is necessary in the case of profiling, or when the processing of sensitive data is happening on the large scale, or if there is a "systematic monitoring of public areas on a large scale" [56] is going on.

Art.35, Art.36 Rec:(84), (89), (90), (91), (92), (93), (94),(95), (96)

External links:

- EU commission guideline→ link
- Intersoft consulting→ link
- ICO - Data Protection Authority UK→ link

[53] https://ec.europa.eu/info/departments/data-protection-officer$_en$

[54] https://edps.europa.eu/edps-homepage$_en?lang = en$

[55] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item$_id = 611236$

[56] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required$_en$

6 Software Development Life Cycle (SDLC) and GDPR

This section presents tasks in SDLC phases with respect to GDPR requirements. Each stage also includes external resources for detailed instructions for each phase.

6.1 Planning

This stage includes defining and gathering requirement, analysis of the specified requirements and clarifying a plan regarding tasks and resource management towards developing a product.

A software, service or a product is going to be developed. This stage is about understanding the expectations of the product owner, characteristics and functionalities of the product, required resources and overall requirements to achieve the final goal. After defining the requirements, the teams must discuss the feasibility and required actions towards developing the product.

GDPR obligations should be addressed in this stage while defining other requirements. It is relevant to discuss all the defined key topics in this stage particularly personal data, data subjects rights, Privacy by Design, and Data protection impact assessment. Understanding these factors will help the development team to define requirements regarding data protection and information security. For instance, when reviewing the list of key topics, development teams should clearly determine the type of data they are going to collect and process. Or while considering the processing from key topics, the development team must be able to decide on the companies role as a controller, processor or both. Responsibilities defined for each of these roles are different.

After extracting requirements for each phase and key topics, the development team must proper requirement specification document which will be used as a base for the design phase.

The Norwegian Data Protection Authority (DPA) has developed a detailed list of activities for setting requirements which can be accessed here [57].

6.2 Design

The characteristics of GDPR compliant products are going to be defined in the Design stage. The majority of the design specifications in this stage are based on the requirements outlined in the Planning stage.

Design decisions are crucial regarding the management of personal data, so the subsections in Data management topic should be appropriately addressed. Designing software which respects data subject rights is also a major requirement; this includes notifying data subjects about processing, receiving their consent for processing the data and also provide them with controls over their personal data [58]. Privacy by Design is also a repeating requirement which should be addressed during the design phase.

The Norwegian Data Protection Authority (DPA) has developed a detailed list of activities for design related subjects which can be accessed here[59].

6.3 Development

The development stage is about creating the product based on the design specifications, GDPR requirements should have been incorporated to the software design document as well, so the aim is that implementing design specifications based on the regulation requirements will lead to building a GDPR compliant product.

Including data security measures and data, privacy-enhancing technologies such as encryption are relevant topics to discuss during the development phase. Tools, frameworks, protocols and products from third parties should be checked by the development team or the company for following the principle of data privacy and data security.

Regarding the privacy by design topic, Enisa's report [60] is a thorough guide for connecting the legal framework to

[57] https://www.datatilsynet.no/globalassets/global/english/guidelines/privacy-by-design/checklist-requirements.pdf

[58] https://www.mdpi.com/2220-9964/7/11/442

[59] https://www.datatilsynet.no/globalassets/global/english/guidelines/privacy-by-design/checklist-design.pdf

[60] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

the available technologies for building privacy-friendly products.

The Norwegian Data Protection Authority (DPA) recommends secure coding activities [61] and also Provides a checklist [62] for the development phase.

6.4 Test

When the coding is completed, it is time to use various testing methods to assure expected functionalities and design elements. It is also time to test if defined and expected data privacy and data security related matters have been addressed and implemented properly.

A list of possible testing in this stage with respect to privacy and security is listed here [63], check list developed by The Norwegian Data Protection Authority is also available here [64].

6.5 Deployment

Data security, data breach, privacy by design, DPO This stage is about deploying the software in the production environment; the software is fully functional and usable in this stage, therefore, implemented data protection and security means should also be working.

Incident repose plan and security review are the activities that the Norwegian Data Protection Authority (DPA) emphasis on in this stage is available here [65].

6.6 Maintenance

While this stage follows the usual maintenance activities based on the company's maintenance culture and usually focus on implementing changes towards achieving the products that meets all the expected requirements gradually.

Privacy and security are dynamic matters and therefore are in the needs of being discussed and actively attend to, particularly when changes occur, for instance, if the purpose of the personal data collection changes, the content must be updated and the SDLC should go through all the stages for such update. Therefore, all the key topics are relevant to the maintenance stage.

Regular Data privacy impact assessments are crucial in this stage.

The Norwegian Data Protection Authority developed a checklist including some of the important activities for this stage, availble here [66].

[61] https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/?id=7734

[62] https://www.datatilsynet.no/globalassets/global/english/guidelines/privacy-by-design/checklist$_{c}oding.pdf$

[63] https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/?id=7735 by The Norwegian Data Protection Authority (DPA)

[64] https://www.datatilsynet.no/globalassets/global/english/guidelines/privacy-by-design/checklist$_{t}esting.pdf$

[65] https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/?id=7736

[66] https://www.datatilsynet.no/globalassets/global/english/guidelines/privacy-by-design/checklist-maintenance.pdf

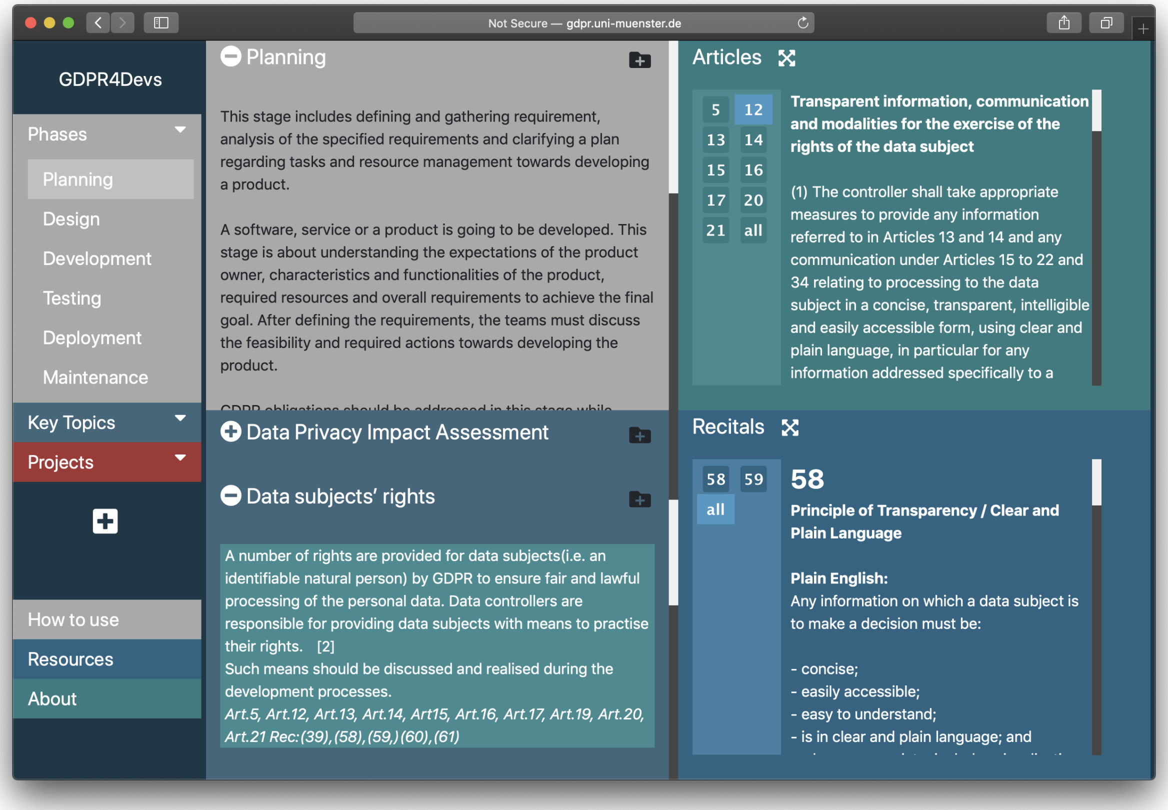
7 Interactive Platform

7.1 Design

An interactive tool was developed to realise the concepts and connections developed in previous sections in a meaningful and useful way.

The platform was designed based on three main characteristics:

- The platform presents complex information on different levels from a general overview to details together with a simplified content.
- The platform links the GDPR requirements to the SDLC phases. The rationale behind building such a connection was to provide developers and designers with the possibility to address privacy-related issues at the same time as tasks relevant to software development stages.
- The platform offers a project feature that can keep tracks of privacy-related tasks. This feature allows users to select relevant important aspects in each phase in order to address them systematically.



This stage includes defining and gathering requirement, analysis of the specified requirements and clarifying a plan regarding tasks and resource management towards developing a product.

A software, service or a product is going to be developed. This stage is about understanding the expectations of the product owner, characteristics and functionalities of the product, required resources and overall requirements to achieve the final goal. After defining the requirements, the teams must discuss the feasibility and required actions towards developing the product.

GDPR obligations should be addressed in this stage while

A number of rights are provided for data subjects(i.e. an identifiable natural person) by GDPR to ensure fair and lawful processing of the personal data. Data controllers are responsible for providing data subjects with means to practise their rights. [2]
Such means should be discussed and realised during the development processes.
Art.5, Art.12, Art.13, Art.14, Art15, Art.16, Art.17, Art.19, Art.20, Art.21 Rec:(39),(58),(59,)(60),(61)

Transparent information, communication and modalities for the exercise of the rights of the data subject

(1) The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a

58

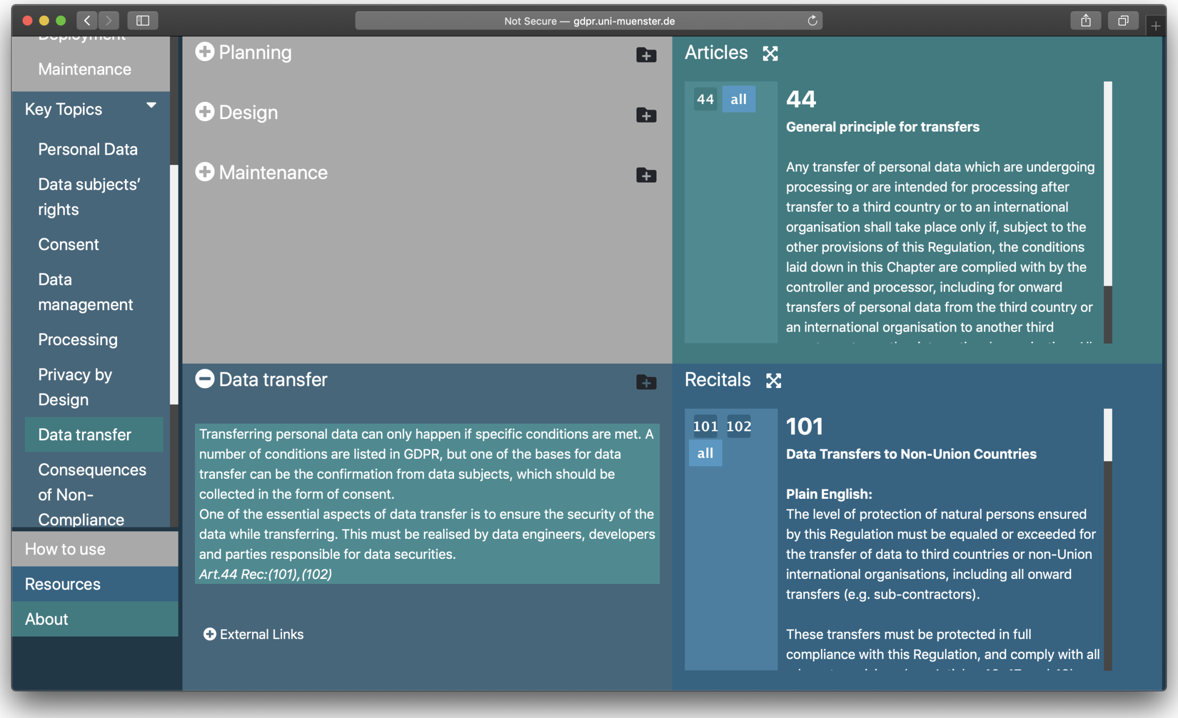
Principle of Transparency / Clear and Plain Language

Plain English:
Any information on which a data subject is to make a decision must be:

- concise;
- easily accessible;
- easy to understand;
- is in clear and plain language; and

Figure 2: Guideline screenshot

The platform also provides an index to relevant external links, including other guidelines, materials and products developed to help with understanding GDPR requirements or fulfilling such requirements. A demo of the platform has been made publicly available from June 2019 and is available at gdpr.uni-muenster.de. The content and the features of the platform has been developed to support simplicity, flexibility, and smooth user interaction. We followed usage-centred approach and focused on a few scenarios that potential users could interact with the website.



Transferring personal data can only happen if specific conditions are met. A number of conditions are listed in GDPR, but one of the bases for data transfer can be the confirmation from data subjects, which should be collected in the form of consent.
One of the essential aspects of data transfer is to ensure the security of the data while transferring. This must be realised by data engineers, developers and parties responsible for data securities.
Art.44 Rec:(101),(102)

44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third

101

Data Transfers to Non-Union Countries

Plain English:
The level of protection of natural persons ensured by this Regulation must be equaled or exceeded for the transfer of data to third countries or non-Union international organisations, including all onward transfers (e.g. sub-contractors).

These transfers must be protected in full compliance with this Regulation, and comply with all

Figure 3: Guideline screenshot

While the demo is available through the mentioned URL, the web application of the platform has developed to be available for download and installation (i.e. brief explanation of the technical aspects are explained in section 7.4, and the web application is available through a link [67].

7.2 Content

The content of the platform presents the information from the GDPR original document in an understandable and accessible way. Therefore, the information presented in the first five chapters of GDPR has been selected and summarised to ten important key topics. The reason for focusing on only the first five chapters was that the remainder of the chapters were not relevant to the SDLC phases, and they did not apply to development processes.

The content created for the platform is the combination of 1) text directly from the GDPR document (i.e. Articles and Recitals - as presented in section 5), 2) explanatory sources such as materials that data protection authorities (DPAs) have provided in different states for specific purposes, for instance, the guideline uses external links to detailed tasks list for each software development phase, which is created by Norwegian DPAs [68], as shown in section 6 and 3) information created by individuals working towards making GDPR understandable for public [69]. The platform uses the latter in plain English section of the recitals to provide a simpler version of the recital explanation before presenting each recital's original description.

The platform presents SDLC phases with a short description in the context of privacy protections. When a stage is selected, a list of corresponding key topics is also shown to point out at important general aspects that are needed to be considered in each SDLC phase. Detailed practical instructions are listed as external links in the description

[67] http://gdpr.uni-muenster.de/download$_a pplication$
[68] https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/
[69] https://www.davidfroud.com/free-resource-the-gdpr-in-plain-english/

of each stage. Articles and recitals, together with a simplified version of the recitals, are also part of the platform's content.

Summarising the content of five chapters provides an overview of the important topics that those involved in design and development of a software which deals with the collection, process or storage of personal data should be familiar with and have a general understanding about. The key topics are presented in the guidelines with a short description and relevant links to further explanations. The description and the external links are limited to the context of software development processes.

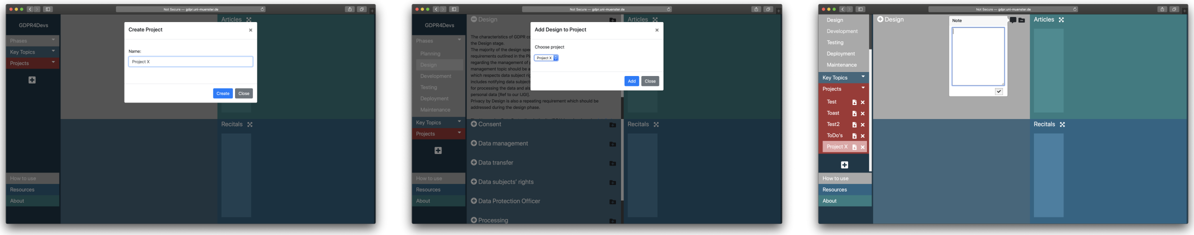
It is essential to clarify that the selection of the content, especially for key-factors is just one example of the relevant and important topics to SDLC, this content can be changed and adjusted based on project's goal by developers team through the installed application. The technical requirements are briefly explained in section 7.4.

7.3 Interactive Features

While the primary goal of the guideline is to present the information in an understandable way, the secondary goal is to show that information with connections and links to SDLC. As explained earlier, the rationale behind building such a connection was to integrate the privacy-related tasks into the rest of the tasks developed in various phases of software development. For instance, the tasks of defining and analysing GDPR requirements can be assigned and examine at the same time that developers and designers are developing general requirements at the beginning of the development process. But the more detailed and specific tasks can also be followed when the team proceed in further stages, for example, one can discuss how to design the user interface (UI) of a consent form while making a decision regarding the other UI aspects of the software in the Design phase.

The layered presentation of the connected content is also one of the factors that have been thought thoroughly, at any moment, the user has the possibility of an overview during her interaction with the guideline apart from its starting point. Meaning that, if user selects a key topic such as personal data, phases relevant to that key topic together with related articles and their explanations as recitals will be accessible at the same time and in one page, for more detailed view in each of these sections, suitable UI has been designed to provide more in-depth and comprehensive level of information presentation which are the corresponding articles to each key topics and also simple explanation of the recitals and their original descriptions.

In addition to the presentation of the connected and relevant information in one page, in order to address the issue of keeping tracks of privacy-related activities, the platform provides users with the option of 'create project'. The user can create and customise this feature based on the project she is working with. This option allows the user to select the desired content from the platform. For instance, if the development team is currently in the design stage, they have the possibility to choose from seven key topics, they can select the factor that is going to be discussed, addressed or implemented. This feature is specifically designed to help developer and designers to keep track of the tasks and requirements relevant to their software or products; they can also keep tracks of the specific actions linked to those requirements or any other type of note desired. Eventually, they can export their customised project, including required legal information, specific tasks needed to fulfil those requirements or action that took place in the compliance process. The data generated in this section will be stored locally on users' devices due to possible privacy-related concerns. This feature is valuable on both individual and team levels for organising the tasks, but it can also be useful during the audits or DPIAs.



Create Project

Name: Project X

Add Design to Project

Choose project: Project X

Figure 4: Create Project feature example, creating the content and adding note features

7.4 Technologies

The application is based upon the modern web technologies JavaScript and Node-JS, using KeystoneJS, Pug, jQuery and Bootstrap as main frameworks. It uses the NoSQL database MongoDB. Due to the assumed use cases the application is currently not adjusted for smartphone usage.
The application provides a content management system (CMS), completely available at client-side. Developer team can edit all contents, including the texts of dev-phases, key topics, articles and recitals. However, changes in the CMS should be done carefully. More information on how to use the CMS are provided in the 'readme' file of the application.
The application is meant to be installed on the servers of the companies. Installation instructions are also provided in the 'readme' text file. Installation is possible by manual installation or in a docker-container. In both cases, installation should be easy to manage and not consuming a lot of time. In case of the docker container the database will run inside the container, for manual installation there is a need to start the database manually on the machine.
The application will match exactly the demo available at gdpr.uni-muenster.de and is availbe for download at ... .

8 Discussion

8.1 Implications of Introducing GDPR to Development Teams

For many years, software development teams did not actively address privacy-related issues as part of their processes while developing services. While this might be still true in some cases, it is not that easy to avoid addressing privacy-related matters due to many reasons; From one hand consumers' awareness and concerns have increased regarding the consequences of using technologies that can lead to privacy and safety risks. Events such as Snowden revelation about US government massive data collection programs helped to increase awareness of the public regarding the importance of data protection. On the other hand, some governments who are more responsible for protecting their citizens' privacy have taken actions and have established new regulations that obligate technology and service providers to respect consumers' rights about the protection of their data.

Legal obligations are one of the effective practices that can ensure the privacy protection of individuals. Nevertheless, the gaps between legal and technical world stand as one of the main obstacles for the implementation of such regulations. As a general observation, developing products with balanced features which support requires a group effort meaning that stakeholders with various skills such as service providers, user experience designers, lawyers, privacy experts, product owners, etc. should collaborate with developers and designers to ensure the functionally- privacy balance for developing GDPR compliant product. It is also relevant to point at the current business practices that are based on targeting advertisements through profiling or clustering users without their knowledge should go through fundamental changes in order to support transparency and trust.

8.2 Limitations

It's important to mention that the platform developed in this project can not guarantee that the resulting products are GDPR compliance as every product has unique characteristics and requirements, so while the platform can help developers team to some extent, there is always a good idea to discuss privacy-related issues with a group of expert to ensure the compliance.

Also while the platform redirects users to set of instructions developed by authorities, it does not provide practical instructions for developers group as every product, based on their functionality and nature must be analysed and developed by the development team to extract required steps for developing a GDPR compliant product.

8.3 Future Research

Further research and studies are needed to explore the topic of providing practical instructions based on legal requirements and integration of such instruction into the development processes of products in the context of personal data protection.

While SDLC has been established a set of standards in the process of software development which is flexible enough to be used by the majority of the development teams, there is a need for developing similar standards for legal and privacy-related based requirements in the same context. Another area that is in the need of further exploration is about education various stakeholders not only about the requirements but also societal reasons of benefits of protecting individuals privacy to build a future which is not in the danger of digital dictatorship.

On a more detailed level, key topics that were selected in this research and also in the platforms are limited to our research perspective regarding essential factors, and there is a need for further discussions towards confirming these key topics and also extending the list. In general, it is important to explore difficulties that developers teams might face while addressing privacy-related issues and also explore various solutions for such difficulties to eventually build tools, frameworks and standard cycles for development teams to use when addressing privacy-related matters.

8.4 Summary

This research aimed at examining the gap and challenges that the introduction of GDPR has caused for software development teams. After gathering insights regarding current difficulties, this research systematically analysed the legal text and developed a connection between essential topics in GDPR requirements and SDLC. Eventually, for realising these connections in a meaningful way, this research developed a platform to provide a way to integrated GDPR requirements into the SDLC with the goal of facilitating the accessibility of legal documents. This platform includes features to help development teams keep tracks of GDPR related tasks. The platform particularly focuses on facilitating the understanding of the GDPR requirements. The platform categorises the key factors from the GDPR document. One has the possibility to go through the general description of these factors, but also if one is interested in detailed articles and recitals can have easy access to such information.

Our results can help service providers, software developers and designers to comply with the GDPR through one platform. Our platform provides integration of GDPR requirements to the software development phases.

A First Appendix - Existing solutions

List of the companies producing privacy management tools and the features they provide:

1. Aptible Inc. Assessment Manager, Data Mapping, Incident Response.
2. AuraPortal. Assessment Manager, Consent Manager, Incident Response, Privacy Information Manager.
3. Avepoint Activity Monitoring, Assessment Manager, Consent Manager, Data Discovery, Data Mapping, De-identification/Pseudonymity, Incident Response, Privacy Information Manager, Website Scanning.
4. CENTRL Inc Activity Monitoring, Assessment Manager, Consent Manager, Data Discovery, Data Mapping.
5. Clarip Assessment Manager, Consent Manager, Data Discovery, Data Mapping, Website Scanning.
6. ClearSwift Activity Monitoring, Data Mapping, Incident Response.
7. Compliance Technology Solutions B.V. Assessment Manager, Data Mapping, Incident Response.
8. Compliancelog Consent Manager, Data Mapping, Incident Response.
9. CompLions-GRC BV Activity Monitoring, Assessment Manager, Data Discovery, Data Mapping, Incident Response.
10. CUBE Activity Monitoring, Assessment Manager, Data Mapping, Incident Response, Privacy Information Manager.
11. Data Solver Assessment Manager, Consent Manager, Data Mapping, De-identification/Pseudonymity.
12. Dataguise Activity Monitoring, Assessment Manager, Data Discovery, Data Mapping, Incident Response, Privacy Information Manager.
13. datastreams.io Assessment Manager, Consent Manager, Data Mapping.
14. Didomi Assessment Manager, Consent Manager, Website Scanning.
15. DLP Assured Activity Monitoring, Assessment Manager, Consent Manager, Data Discovery, Data Mapping.
16. Draftit Privacy Activity Monitoring, Assessment Manager, Data Mapping, Incident Response.
17. DSS Consulting Ltd. Activity Monitoring,, Assessment Manager, Consent Manager, Data Discovery, Data Mapping, Incident Response.
18. eDatask Assessment Manager, Consent Manager, Data Mapping.
19. HexaTier Activity Monitoring, Data Discovery, De-identification/Pseudonymity.
20. Immuta Activity Monitoring, Data Discovery, Data Mapping, De-identification/Pseudonymity.
21. Information First Data Discovery, Data Mapping, De-identification/Pseudonymity, Privacy Information Manager.
22. Integris Activity Monitoring, Assessment Manager, Consent Manager, Data Discovery, Data Mapping.
23. The media Trust Activity Monitoring, Data Discovery, Incident Response.
24. MEGA International Assessment Manager, Consent Manager, Data Mapping, Incident Response.
25. Mentis Activity Monitoring, Data Discovery, De-identification/Pseudonymity.
26. Meta Compliance Assessment Manager, Data Mapping, Incident Response.
27. Mighty Trust Limited Activity Monitoring,Assessment Manager, Data Mapping, Incident Response, Privacy Information Manager.
28. NextLabs,Inc. Activity Monitoring, Data Discovery, Data Mapping, Enterprise Communications, Privacy Information Manager.
29. Nymity Assessment Manager, Data Mapping, Privacy Information Manager.
30. OneTrust Assessment Manager, Consent Manager, Data Discovery, Data Mapping, Incident Response, Privacy Information Manager, Website Scanning.

31. OptInsight Activity Monitoring, Consent Manager, Data Discovery
32. Privacy Lab Activity Monitoring, Assessment Manager, Consent Manager, Data Mapping.
33. Privitar Assessment Manager, De-identification/Pseudonymity, Privacy Information Manager.
34. Proofpoint Activity Monitoring, Data Discovery, Data Mapping, Incident Response.
35. Proteus-Cyber Ltd Activity Monitoring, Assessment Manager, Consent Manager, Data Discovery, Data Mapping, Incident Response.
36. Qixium Data Discovery, Data Mapping, De-identification/Pseudonymity.
37. SAS Global Data Management Activity Monitoring, Data Discovery, De-identification/Pseudonymity.
38. Secupi Activity Monitoring, Consent Manager, Data Mapping, De-identification/Pseudonymity.
39. Sensorpro Assessment Manager, Consent Manager, De-identification/Pseudonymity.
40. Senzing Assessment Manager, Consent Manager, Data Discovery, Data Mapping.
41. SkyHigh Activity Monitoring, Data Mapping, Incident Response.
42. Signatu Assessment Manager, Consent Manager, Data Mapping
43. Smart Privacy Assessment Manager, Consent Manager, Data Mapping, Incident Response, Privacy Information Manager.
44. Spearline Risk and Compliance Assessment Manager, Consent Manager, Data Mapping, Incident Response.
45. Stratrai Ltd. Assessment Manager, Consent Manager, Data Mapping, Incident Response, Privacy Information Manager.
46. Structure Systems Data Discovery, Data Mapping, De-identification/Pseudonymity.
47. SureCloud Activity Monitoring,Assessment Manager, Data Mapping, Incident Response, Privacy Information Manager.
48. Systnaps Data Discovery, Data Mapping, De-identification/Pseudonymity.
49. T Closeness Consent Manager, Data Discovery, Data Mapping.
50. Transcend Activity Monitoring, Assessment Manager, Consent Manager, Data Discovery, Website Scanning.
51. TrustArc Assessment Manager, Consent Manager, Data Mapping, Website Scanning.
52. Trust-Hub Activity Monitoring, Consent Manager, Data Mapping
53. Usoft Activity Monitoring, Assessment Manager, Consent Manager, Data Mapping, Incident Response
54. Veritas Activity Monitoring, Data Discovery, Data Mapping, Incident Response.
55. WireWheel.io Activity Monitoring, Assessment Manager, Consent Manager, Data Discovery, Data Mapping

B Second Appendix - Survey questions

GDPR Survey

The General Data Protection Regulation (GDPR) is designed to harmonised data protection regulations across Europe. GDPR provide better control over EU citizens’ personal data. Therefore, everyone who is involved in collecting, holding using or processing the personal data of individuals (employees or customers or both) must comply with the regulations.

This project is funded by Förderverein des Instituts für angewandte Informatik. Answering the following questions will be important to understand which aspects of GDPR is challenging for you. The goal of this survey is to find out the difficulties that you have encountered while addressing GDPR requirements. The ultimate goal of this project is to design guidelines that can facilitate the process of becoming GDPR compliant for you, particularly during the software development processes.

We are focusing on developing a guideline that can be useful for those who are going to implement practical means to achieve GDPR compliance. Therefore, the best person/s to answer this survey are developers or designers who are involved in the GDPR compliance process. Nevertheless, we would appreciate everyone's participation engaged in the GDPR compliance process in your company. Please sign the consent form before answering the survey. We are not going to associate any personally identifiable information or the name of your company to the survey responses.

1. **Your job title:**
   please also specify your role regarding data protection compliance if applicable

2. **How many individuals are responsible for complying with data protection regulations in your company?**

3. **Regarding the compliance with GDPR, our company:**
   Mark only one oval.

   ○ has not implemented or planned any activities yet
   ○ has partially implemented or planned some activities
   ○ has successfully implemented all the GDPR requirements
   ○ Is not going to comply with GDPR
   ○ I do not know the answer

4. **How do you manage tasks regarding GDPR?**
   (please include the name if it is applicable)
   Mark only one oval.

   ○ Manually (e.g. excel sheets or other means) : ....
   ○ Software developed only to use inside our company: ....
   ○ Commercial software (e.g. developed by third parties): ....
   ○ A consultancy firm or an agency or another company: ....
   ○ I do not know the answer
   ○ Other:

5. **How would you describe your company's role based on data protection definition?**
Mark only one oval.

○ We are data controller
○ We are data processor
○ We are both data controller and data processor
○ I do not know the answer

Instructions

Please fill the gaps in the following statements based on the level of difficulties you have experienced or are experiencing in the process of complying with the general Data Protection Regulation (GDPR). If you are involved in any software development processes and have or had to consider GDPR compliance, please have that process in mind while choosing the answers, otherwise please select the answers generally. There might be statements that your company has not started to address yet. For those statements, please consider the anticipated level of difficulty. If you do not choose any level, we will assume that you did not know the answer. The level of difficulties has been defined as (1) easy, (2) moderately easy, (3) moderately difficult, and (4) difficult.

6. **I find the understanding of GDPR requirements ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

7. **I think finding guidelines, instructions, tools or proper resources for becoming GDPR compliant is ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

8. **I think mapping out the data flow in our company is ... .**
(i.e. to identify the flow of the data inside and outside of our company)
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

9. **While collecting different types of data, I find understanding which is categorised as personal data is ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

10. **I find documenting the information about the collected personal data such as its source or the period that the data is going to be kept ... .**

(i.e. according to GDPR, the reason for holding the personal data, the period that data is going to be kept, … should be documented)

Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

11. **The collected personal data could be processed for different reasons, I find explaining those reasons to others ... .**

(i.e. according to GDPR, the purpose of the processing should be clarified)

Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

12. **I think providing means for data subjects (users/customers) to exercise their rights is … .**

(i.e. data subjects are any individual who can be identified through collected data about them . According to GDPR, data subjects rights includes : the right of access, the right to rectification, erasure, and restrict processing)

Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

13. **I find providing our customers/ end users with the personal data collected about them in the case of a request ... .**

Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

14. **I find explaining to customers/ end users why we are collecting their personal data and what we are going to do with it is ... .**

Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

15. **I find Managing consent forms ... .**

(i.e. includes designing consent forms based on GDPR requirements and also ongoing documentation of the consent forms)

Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

16. **I find managing incidents or data breaches ... .**
(i.e. to know what to do if a data breach occurs and who should be notified).
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

17. **I think securing the collected or processed personal data inside our company ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

18. **I find keeping the personal data secure when sending the data out of the company ... .**
(e.g. for external processing or when there is a need to be transferred to other companies or out of EU)
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

19. **I think performing data protection impact assessment (DPIA) is ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

20. **I think assigning or hiring the right person/s as data protection leads is ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

21. **I find training our staff regarding the importance of complying with the data protection regulations and their responsibilities is ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

22. **I think updating or creating data security and privacy policies based on GDPR is ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

23. **I find keeping track of all the tasks and documentations in the compliance process is ... .**
Mark only one oval.

	1	2	3	4	
easy	○	○	○	○	difficult

Final question

24. **Please mention any tasks or steps, additional to the ones already mentioned, in the process of complying with GDPR that you find challenging or difficult to understand or address.**

25. **Other comments :**

Thank you very much for your time.

Contact person for questions or concerns: Mehrnaz Ataei - Email: m.ataei@uni-muenster.de - Phone: +46707138511

Powered by
Google Forms

C Third Appendix - Survey result

6. I find the understanding of GDPR requirements … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
0.0%	47.1%	47.1%	5.9%	0.0%

7. I think finding guidelines, instructions, tools or proper resources for becoming GDPR compliant is … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
11.8%	29.4%	47.1%	5.9%	5.9%

8.I think mapping out the data flow in our company is … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
17.6%	35.3%	41.2%	5.9%	0.0%

9.While collecting different types of data, I find understanding which is categorised as personal data is … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
29.4%	47.1%	17.6%	5.9%	0.0%

10.I find documenting the information about the collected personal data such as its source or the period that the data is going to be kept … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
0.0%	17.6%	52.9%	29.4%	0.0%

11. The collected personal data could be processed for different reasons, I find explaining those reasons to others … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
17.6%	47.1%	35.3%	0.0%	0.0%

12.I think providing means for data subjects (users/customers) to exercise their rights is ….

Easy	Moderately easy	Moderately difficult	Difficult	blank
0.0%	29.4%	35.3%	23.5%	11.8%

13. I find providing our customers/ end users with the personal data collected about them in the case of a request … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
5.9%	11.8%	52.9%	29.4%	0.0%

14.I find explaining to customers/ end users why we are collecting their personal data and what we are going to do with it is … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
29.4%	47.1%	23.5%	0.0%	0.0%

15.I find Managing consent forms … .

Easy	Moderately easy	Moderately difficult	Difficult	blank
5.9%	29.4%	41.2%	17.6%	5.9%

16.I find managing incidents or data breaches ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
5.9%	41.2%	47.1%	5.9%	0.0%

17.I think securing the collected or processed personal data inside our company ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
17.6%	64.7%	11.8%	5.9%	0.0%

18.I find keeping the personal data secure when sending the data out of the company ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
17.6%	29.4%	47.1%	5.9%	0.0%

19.I think performing data protection impact assessment (DPIA) is ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
0.0%	5.9%	70.6%	5.9%	11.8%

20.I think assigning or hiring the right person/s as data protection leads is ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
11.8%	35.3%	47.1%	0.0%	5.9%

21.I find training our staff regarding the importance of complying with the data protection regulations and their responsibilities is ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
17.6%	52.9%	17.6%	11.8%	0.0%

22.I think updating or creating data security and privacy policies based on GDPR is ... .

Easy	Moderately easy	Moderately difficult	Difficult	blank
5.9%	29.4%	47.1%	11.8%	0.0%

23.I find keeping track of all the tasks and documentations in the compliance process is ..

Easy	Moderately easy	Moderately difficult	Difficult	blank
0.0%	5.9%	64.7%	29.4%	0.0%

References

[1] Roba Abbas. The social implications of location-based services: an observational study of users. *Journal of Location Based Services*, 5(3-4):156–181, 2011.

[2] EU. Regulation (eu) 2016/679 of the european parliament and of the council - of 27 april 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). 2016.

[3] Yu-Wei Lin. # deletefacebook is still feeding the beast–but there are ways to overcome surveillance capitalism. *The Conversation*, 2018.