WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EQUIS ACCREDITED

Bachelor Thesis

Privacy policies and the GDPR: An Evaluation Framework

Meris Ramic

Subject Area: Information Business

Studienkennzahl: 033/561

Supervisor: Dr. Sabrina Kirrane

Date of Submission: May 02, 2022

Department of Information Systems and Operations, Vienna University of Economics and Business, Welthandelsplatz 1, 1020 Vienna, Austria

DEPARTMENT FÜR INFORMATIONSVERARBEITUNG UND PROZESSMANAGEMENT DEPARTMENT OF INFORMATION SYSTEMS AND OPERATIONS

Contents

List of Figures

List of Tables

Abstract

The popularity of IoT devices, such as fitness trackers, has grown significantly in recent years and is expected to continue to grow in the coming years. The use of fitness trackers led to a multiplication of available personal data. Based on these developments, the EU legislator introduced the General Data Protection Regulation (GDPR) as a safeguard against uncontrolled personal data processing. The introduction of the GDPR resulted in slight improvements regarding the understandability of privacy policies. However, privacy policies in many cases remain complex. In this bachelor thesis, we propose a framework that systematically supports the framework's users to determine whether information relating to the GDPR's material scope and the legal grounds for personal data processing is included.

1 Introduction

The presence of computers of all forms has become ubiquitous in our society. As a consequence of the expanding use of computers in virtually all areas of society, the number of data collected has increased significantly in the course of the past years. While in 2016 an estimate of 6.5 zettabytes of data was generated and processed, this number rose to 64.2 zettabytes for the year 2020 and is expected to rise up to 181 zettabytes in 2025 (Holst, 2021).

The Commission of the European Union (EU Commission) recognised the necessity to amend its regulations regarding the processing of personal data due to the rapid technological progress (Politou et al., 2018). In order to give people more control over their personal data, the Parliament of the European Union passed Regulation (EU) 2016/679, also named the General Data Protection Regulation (GDPR) (Jóri, 2019). The GDPR includes, amongst other principles, a concrete definition on the cases in which the GDPR applies, the so-named material scope. Furthermoe, the GDPR defines under which legal grounds the processing of personal data is considered lawful (Klar & Kühling, 2020; Albrecht, 2019; Frenzel, 2021). Moreover, the EU legislators explicitly mention special categories of personal data and sensitive data in the GDPR which can only be processed based on more stringent legal grounds, as they are considered particularly sensitive in regard to fundamental rights and freedoms (European Parliament and Council, 2016). Special categories of personal data and sensitive data are synonyms and will be used as such in this thesis.

Following the introduction of the GDPR, many companies updated their privacy policies in order to comply with the new regulations set forth in the GDPR (Degeling et al., 2019). Sury (2021) defines privacy policies as a statement disclosing which personal data is processed, why said data is processed and how said data is processed. However, organisations have been criticised for primarily writing privacy policies to safeguard against legal prosecution instead of informing users about data processing activities (Pollach, 2007). Despite recent attempts to make privacy policies easier to understand, complicated, lengthy and technically written legal texts still impede users from obtaining information on the processing of their personal data. Research by Reidenberg et al. (2014) shows that privacy policies are generally considered difficult to understand due to the often complicated and technical language deployed. An investigation conducted by Litman-Navarro (2019) for the New York Times found that privacy policies have improved in terms of readability following the introduction of the GDPR since companies reduced the use of technical jargon. However, the investigator also found that the majority of

people are still not able to comprehend the text presented in privacy policies. Zaeem and Barber (2020) found in their research, including 450 privacy policies, that some privacy policies were not able to comply with all requirements set forth by the GDPR. Research conducted by Linden et al. (2018) found that privacy policies have improved in terms of design and layout after the introduction of the GDPR. However, similar to the findings made by Zaeem and Barber (2020), Linden et al. (2018) conclude that privacy policies often do not include all relevant information foreseen by the GDPR. Mohan et al. (2019) yield similar results in their research on the impact of the GDPR on privacy policies. Due to the difficulty of reading and understanding complex privacy policies, researchers proposed frameworks that can be used on privacy policies in order to review whether the legal requirements set forth by the GDPR are complied with (Lachaud, 2020; Brodin, 2019). However, these frameworks are primarily designed for companies, allowing them to assess whether they are GDPR compliant. Other researchers proposed architectures that enable the development of consumer-oriented automated tools in order to estimate a company's GDPR-compliance (Sánchez et al., 2021; Zimmeck & Bellovin, 2014).

As discussed, the EU legislator considered the increase in personal data processing as a reason to adopt new and stricter regulations on the protection of personal data. A major contributor to the increase in personal data processing is the so-named Internet of things (IoT) devices. IoT devices are generally described as devices that are able to collect and share data with other devices (Dorsemaine et al., 2015). IoT Analytics shows that the number of active IoT device connections, including, e.g., smart home devices and connected cars, was estimated at 11.7 billion in 2020. This number is expected to rise by approximately 265 % to 30.9 billion active IoT device connections for the year 2025 (Vailshery, 2020).

One type of IoT devices that contributes to the increase in personal data processing and that is expected to rise significantly in popularity in the upcoming years due to an increase in health and fitness awareness are fitness trackers (Kao et al., 2019; Koytcheva & Gebbie, 2021). Fitness trackers are wearable health devices that commonly collect personal data, such as the user's heart rate, blood pressure, calories burned, steps taken, hours slept and location (Lee & Lee, 2018; Gabriele & Chiasson, 2020). Forecasts show that the shipments of fitness trackers are expected to rise up to 127 million units in 2025, an increase of approximately 289 % compared to 2018 (Koytcheva & Gebbie, 2021).

The growing popularity of fitness trackers and the accompanying increase in data processing underline the current and future importance of the GDPR and privacy policies for the protection of personal data. These observations highlight the prevailing need for a compact and guiding framework that enables the users of the framework to systematically gather information from privacy policies in order to determine whether and how they may have been influenced by the requirements set forth in the GDPR.

Therefore, the overarching objective of this bachelor thesis is to propose the 'Privacy Policy Appraisal Framework' (PPAF), a framework that supports the framework's users to determine whether the analysed privacy policy includes information on the types and the legal grounds of personal data processing. The use of the PPAF is not limited to one specific user group, as the generic content of the framework allows users from different industries to use the framework. In this thesis, we suggest the following use scenarios: (i) researchers analysing privacy policies, (ii) data subjects collecting information on personal data processing, (iii) companies aligning their privacy policies to GDPR requirements and (iv) the development of privacy policies. Due to our focus on IoT devices, more concretely on fitness trackers and their collection of sensitive data, the PPAF additionally includes the processing of special categories of personal data and explicit consent. Despite our focus on fitness trackers in this thesis, the PPFA's application is not limited to privacy policies from organisations operating in the field of IoT devices. In order to propose said framework, we defined one overarching research question (RQ) and three sub-questions (SQ1, SQ2 and SQ3), namely:

RQ: What aspects does a framework need to include in order to support the framework's users to read and understand privacy policies in relation to the GDPR?

SQ1: How is the definition of personal data, processing of personal data and consent as a legal basis for the processing of personal data to be interpreted in the light of the GDPR?

SQ2: How is information relating to the GDPR's material scope and legal grounds for personal data processing currently disclosed in privacy policies published by companies operating in the field of fitness trackers?

SQ3: What are the necessary steps in order to develop a framework that supports the users of the framework to determine whether information on the GDPR's material scope and legal grounds of personal data processing are included in the analysed privacy policy?

In the following, we briefly present the content of each chapter in this thesis.

In Chapter 2, we present our methodology for the literature review of the GDPR's material scope and the legal grounds for personal data processing. Furthermore, we outline our methodology for the analysis of privacy policies and the development of the PPAF.

In Chapter 3, we discuss the material scope of the GDPR. In order to gather a broad understanding of the material scope, we particularly focus on two terms relevant for the understanding of the material scope, namely personal data and the processing of personal data (Kühling & Raab, 2020). Firstly, we present a literature review on the legal interpretation of the terms personal data and special categories of personal data. In a second step, we review the terms processing of personal data and the means for personal data processing based on primarily legal literature.

Chapter 4 consists of a literature review on the GDPR's legal grounds for personal data processing. Consent is generally considered the main legal basis for companies to process personal data (Krishnamurthy, 2020). Therefore, we particularly focus on a legal literature review of consent as one legal basis for personal data processing and of legal terms associated with consent. Since fitness trackers also collect sensitive data, we additionally review the definitions of explicit consent (Tzanou, 2020).

Based on the literature review in Chapters 3 and 4 of the GDPR's material scope and the legal grounds of personal data processing, we analyse privacy policies in Chapter 5 in order to study whether the privacy policies may have been influenced by the GDPR. The analysis is conducted on six privacy policies published by companies operating in the field of fitness trackers. More concretely, based on our analysis in Chapter 5, we want to answer whether privacy policies mention the types of personal data and special categories of personal data that are processed, the purposes for personal data processing, and consent and explicit consent as legal grounds for personal data processing. Chapter 5 concludes with an analysis of the terminology used in the privacy policies. More specifically, we analyse whether terminology used in the GDPR is mirrored in privacy policies.

In Chapter 6, we present PPAF, a framework that enables the framework's users to assess whether the GDPR may have influenced privacy policies. The

literature review in Chapters 3 and 4 and the subsequent analysis of privacy policies in Chapter 5 lead to the identification of several parameters that allow users of the framework to determine whether the analysed privacy policy includes information regarding the GDPR's material scope and the legal grounds for personal data processing. Furthermore, the PPAF enables the users to evaluate the display and understandability of privacy policies.

Finally, in Chapter 7, we discuss the limitations of our approach and suggest possible further development of our analysis and the PPAF for future work. Lastly, we summarise the findings of our literature review on the GDPR's material scope and legal grounds for personal data processing, our analysis of privacy policies and our proposed framework.

2 Methodology

From a methodological point of view, this bachelor thesis is structured in three parts, as summarized in Figure 1:

(1) In a first step, we present our findings on the legal definitions for the GDPR's material scope and the legal grounds for personal data processing based on a literature review. This approach applies particularly to Chapters 3 and 4 of our thesis.

(2) Subsequently, we analyse six privacy policies in order to determine whether information regarding the GDPR's material scope and the legal grounds for personal data processing are mentioned in the privacy policies based on a case study analysis. For this thesis, the privacy policies represent the cases of our case study.

(3) Finally, we develop PPAF, a framework that allows the framework's users to systematically analyse whether information on the GDPR's material scope and legal grounds for personal data processing is mentioned in the privacy policy. We based the development of the PPAF on our literature review in Chapters 3 and 4 and our analysis of privacy policies in Chapter 5.

In the following subchapters, we present a theoretical background on each methodology applied in this thesis and subsequently elaborate on why we chose the respective methodology and how the methodology was applied concretely in this thesis.

2.1 Literature review

Firstly, we aimed at reviewing current definitions for the terms related to the GDPR's material scope and the legal grounds for personal data processing. The review of the concrete meaning of the terms served as the basis for the development of our proposed framework. Since our goal was to generate a framework based on the insights from a literature review, we chose an integrative literature review as our research method. Torraco (2005) describes an integrative literature review as a research method that enables its users to incorporate the findings from the literature review into new frameworks and models for the analysed topic.

For our literature review, we primarily focused on legal literature related to the GDPR. A major part of legal studies and literature consists of legal interpretations. A legal interpretation aims to derive a precise understanding of legal terms and texts (Soames, 2011). As we aimed to gather an understanding of the terms related to the GDPR's material scope and legal

Figure 1: Research methods applied in this thesis

grounds for personal data processing, we considered the review of legal literature and its legal interpretations to be the adequate method to achieve said goal. Since the EU legislators enacted the GDPR, we predominantly focused on legal literature from within the EU. More concretely, we focused on German and Austrian legal literature. The reason to primarily focus on German and Austrian legal literature is a long-standing tradition in German-speaking countries to provide comments on a legal text in a very detailed manner (Zimmermann, 2020). According to Kästle-Lamparter (2016), comments are based on legal texts and extensively elaborate on the meaning of the terms mentioned in the text. According to Zimmermann (2020), the practice of comments is well-established in German-speaking countries, as both legal scholars from academia as well as practicing lawyers compose legal comments. Legal comments are commonly cited in jurisprudence in German-speaking countries and generally enjoy high importance among legal scholars. Based on research by Zimmermann (2020), Spain and Italy are other countries of the European Union where the concept of comments is similar to German-speaking countries. However, in Spain and Italy, comments do not have such an important meaning and were therefore not considered in our literature review. Other countries from the EU either are not familiar with the concept of comments according to the definition by Kästle-Lamparter (2016) or we could not access the literature due to a language barrier.

Based on our decision to primarily use German and Austrian legal literature in order to review definitions for the GDPR's material scope and legal grounds for personal data processing, we predominantly searched legal databases to obtain the required information, namely: Beck-Online[1],

[1]https://beck-online.beck.de/Home

EUR-Lex[2], HeinOnline[3], JSTOR[4], Juris[5], Lexis 360[6], SSRN Social Science Research Network[7], Statista[8] and Westlaw International[9]. The databases mentioned were browsed using search terms related to the GDPR's material scope and legal grounds for personal data processing, such as: 'material scope GDPR', 'personal data GDPR', 'consent GDPR', 'automated processing GDPR', 'GDPR legal grounds for personal data processing', and variations thereof. Only articles that included a discussion on the interpretation of the terms mentioned in the GDPR were considered for this part. The interpretation of terms in a legal context requires specific skills and is subject to certain rules (Soames, 2011). As legal scholars are extensively concerned with these aspects, only articles published by legal scholars were considered. These papers had to include, alternatively, (i) concrete examples of how the terms are to be understood, (ii) a references to current jurisprudence indicating how the scope of the considered term is currently defined or (iii) a reference to other legal regulations that elaborate the interpretation of the respective term.

Our literature review led to the identification of concrete terms related to the GDPR's material scope and legal grounds for personal data processing. For the GDPR's material scope, we considered the following terms: 'personal data', 'special categories of personal data', 'data processing' and 'means of data processing'. Our research showed that some data processed by fitness trackers is considered personal data. Furthermore, we discovered that some data processed by fitness trackers are regarded special categories of personal data by the GDPR. Therefore, we additionally included the term special categories of personal data in our thesis. Moreover, we conducted a review on the interpretations of the legal definition of data processing according to the GDPR since our topic evolves around the processing of personal data.

Regarding the GDPR's legal grounds for personal data processing, we focused on the following terms: 'consent', 'freely given consent', 'specific consent', 'informed consent', 'unambiguous agreement to personal data processing' and 'explicit consent'. Our research showed that consent is the main

[2]https://eur-lex.europa.eu/homepage.html?locale=en
[3]https://home.heinonline.org/
[4]https://www.jstor.org/
[5]https://www.juris.de/jportal/nav/index.jsp#/
[6]https://360.lexisnexis.at/
[7]https://www.ssrn.com/index.cfm/en/
[8]https://www.statista.com/
[9]https://www.westlawinternational.com/

legal basis for personal data processing for companies operating in the field of fitness trackers (Krishnamurthy, 2020). Therefore, we primarily focused on consent as a legal ground for personal data processing. In Art. 4(11) GDPR, the EU legislator sets out four requirements that must be fulfilled to consider consent validly obtained: consent has to be *"[...] freely given, specific, informed and [...]"* unambiguously agreed to. Thus, we reviewed the definitions and comments provided by legal scholars on the mentioned requirements. Furthermore, we included explicit consent. As mentioned, fitness trackers often collect data considered sensitive data. As fitness trackers collect sensitive data, we added explicit consent as a legal ground for sensitive personal data processing to our literature review. Based on our specific focus on consent as a legal ground for personal data due to its importance, we exclusively considered explicit consent and excluded other legal grounds for the processing of sensitive data (Krishnamurthy, 2020).

2.2 Case study analysis

In a second step, we aimed to analyse how companies currently disclose information on the processing of personal data, with a particular focus on the GDPR's material scope and the legal grounds for personal data processing. Such information is commonly published in privacy policies (Sury, 2021). In order to gather an understanding of how this information is displayed, we decided to analyse privacy policies based on a collective case study analysis (Stake, 1999; Yin, 2014).

Case study analysis describes research that gathers information on the research subject by analysing one or several real-life cases (Crowe et al., 2011). More concretely, in a collective case study, researchers analyse several cases of the respective research subject to find similarities and differences in the cases in order to derive more generally applicable patterns about the analysed research subject (Stake, 1999). For our collective case study research, we roughly followed the structure suggested by Crowe et al. (2011), namely: case definition, case selection and data collection, analysis and interpretation.

Case definition. Firstly, we defined the scope of the case. As this thesis primarily considers the GDPR's material scope and legal grounds for personal data processing, our research regarding currently published privacy policies was limited to the analysis of privacy policies' information on the material scope and lawfulness of personal data processing. More concretely, during our literature review, we identified several terms related to the GDPR's material scope and legal grounds for personal data processing. Based thereupon, we included four aspects in our case study, whereby we wanted to analyse whether the privacy policies included information on those aspects, namely:

(1) types of personal data processing, (2) special categories of personal data, (3) purposes for personal data processing and (4) consent and explicit consent as a legal ground for personal data processing. Additionally, we aimed at analysing whether privacy policies mirrored the terminology set forth by the GDPR. Hence, our case study research included the aspect (5) terminology of privacy policies.

Case selection. In a second step, we chose the privacy policies for our analysis. In our research, we focused on data processing by fitness trackers. Consequently, we considered only privacy policies published by companies that offer fitness trackers in their product range for our case study. Moreover, we aimed at studying whether information on the GDPR's material scope and legal grounds for personal data processing in privacy policies vary based on the company's location. Hence, we included companies from three continents, namely Europe, America and Asia that sell their products to the EU market. The deciding criteria for including a company's privacy policy in the case study analysis were the fitness tracker's functionalities. We consulted the company's official websites and identified six companies that offer at least one fitness tracker with identical product functionalities. Three pairs out of the six selected companies are headquartered in Europe, America and Asia.

Data collection, analysis and interpretation. The aim of the analysis was not the assessment of the privacy policies but rather the documentation of whether information on the identified aspects in the *case definition* is included. In order to determine whether privacy policies included such information, we conducted a conceptual content analysis (Columbia Mailman School of Public Health, n.d.). Conceptual content analysis is defined as analysing whether certain aspects can be found in the analysed subject or not (Columbia Mailman School of Public Health, n.d.). The identified aspects (1) to (4) in our *case definition* were analysed thematically, i.e., we did not search for the inclusion of certain words or phrases in the privacy policies, but whether the information on the identified aspects was generally provided. The criteria to consider the analysed aspect as included or not stems from our review of interpretations for the regarded aspect. However, in the case of the analysis of the terminology of privacy policies, we reviewed the privacy policies for the existence of concrete words. Since our analysis consisted of explicitly only investigating whether certain information or words were provided in the privacy policies, we developed the following interpretation of the results: the information is either included (✓) or not included (—). Privacy policies that provide only partial or contradictory information are marked with a swung dash (∼).

2.3 Framework development

Finally, we developed a framework that stems from our literature review and our case study analysis. The PPAF enables the framework's users to systematically identify whether information on the GDPR's material scope and legal grounds for personal data processing is mentioned in the analysed privacy policies. As highlighted by other researchers, there is no standard methodology for developing frameworks (McMeekin et al., 2020). Research by McMeekin et al. (2020) showed that in most cases, frameworks are developed based on methods used by other researchers. The methodology for developing the PPAF was primarily based on the procedure applied by Squires et al. (2016) and Brodin (2019). Squires et al. (2016) conducted a literature review in order to identify the challenges in currently implemented public health economic models. The identification of challenges sets the scope of the framework. Our literature review led to the identification of terms related to the GDPR's material scope and legal grounds for personal data processing. The identified terms predominantly reasoned the content and scope of the PPAF. Moreover, based on the literature review, we were also able to incorporate the theoretical background regarding the legal interpretation of the identified terms into our framework. However, we additionally aimed to include the status-quo of how companies disclose information regarding the GDPR's material scope and legal grounds for personal data processing. Hence, we additionally incorporated insights from our case study analysis into the PPAF. The inclusion of current practises into frameworks stems from the research conducted by Brodin (2019). Brodin (2019) developed a GDPR-compliance framework for small- and medium-sized enterprises. During the development of the framework, Brodin (2019) worked together with staff from small- and medium-sized enterprises in the form of interviews and workshops in order to assess how enterprises currently implement processes to the GDPR. In our collective case study analysis, we evaluated privacy policies published by companies operating in the field of fitness trackers in order to determine how information regarding the GDPR's material scope and legal grounds for personal data processing are currently disclosed. Thereby, we identified whether said information is included and additionally how said information is presented. The proposed PPAF, thus, contains the theoretical background on the identified terms based on our integrative literature review and is supplemented by the current status-quo of information disclosure in privacy policies.

3 The material scope of the GDPR

The GDPR was introduced by the European Parliament and the Council of the European Union with the aim to give people more information on who processes their personal data and for which reasons their personal data is processed (European Parliament and Council, 2016). The Data Protection Directive, a predecessor of the GDPR, was considered outdated and insufficient to meet the challenges presented by the rapid advancements in the field of data processing (Politou et al., 2018). Due to the EU's high standards concerning data privacy and protection, as it considers these from a human right's perspective, the European Commission, the European Council and the European Parliament recognized the necessity of a revised, more modern, uniform and up to date regulation of data privacy and data protection (European Parliament and Council, 2016; Mesarčík, 2020). The development of the legal text of the GDPR was substantially influenced by the Charter of Fundamental Rights of the European Union (CFR), more concretely by Art. 8(1) CFR (Mesarčík, 2020). This article states that *"[e]veryone has the right to the protection of personal data concerning him or her"* (European Parliament, the Council and the Commission, 2012). The European legislator accentuated on the human right's perspective even further in Art. 1(2) GDPR, stating that the *"[...] Regulation protects fundamental rights and freedoms of natural persons [...]"*. Based on these legal foundations, the GDPR was negotiated for several years by representatives from different national and EU institutions, such as the European Commission, the European Council, the European Parliament and the European Data Protection Supervisor, before being approved by the European Parliament on April 14th, 2016 (European Parliament, 2016; European Data Protection Supervisor, n.d.). Approximately two years later, on May 25th, 2018, the GDPR came into force (Voigt & von dem Busche, 2018).

In the following subsections, we discuss the material scope of the GDPR in order to gather information on the (potential) appliance of the GDPR in the case of data processing by fitness trackers. The analysis is conducted based on legal comments from, inter alia, legal scholars and EU legislators on the terms set forth in the GDPR. A legal comment offers detailed explanations of the legal text of a specific article, often including references to other articles and case law which clarify the abstract meaning of the respective article (Zimmermann, 2020).

In general, the material scope defines which processing activities are to be considered subject to the GDPR. More concretely, Art. 2(1) GDPR indi-

cates the activities and processes that the GDPR regulates, as it states the following: *"This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system"*, while Art. 2(2) provides activities that exempt the application of the GDPR. In order to gather a comprehensive understanding of the meaning of Art. 2 GDPR, a more detailed analysis of the terms mentioned in Art. 2 GDPR will be conducted in the following sections. For the purpose of ensuring clear and uniform interpretation of the vocabulary in the GDPR, the legislator provided legal definitions for some of these terms under Art. 4 GDPR. However, terms that are not considered under Art. 4 GDPR may be elaborated more concretely in the recitals of the GDPR or have to be derived from other laws, jurisprudence and legal literature.

3.1 Personal data

Personal data, as defined under Art. 4(1) GDPR, *"[...] means any information relating to an identified or identifiable natural person ('data subject') [...]"*. Art. 4(1) GDPR further elaborates on the meaning of an identifiable natural person, who is hereinafter, in coherence with the GDPR, referred to as a data subject. A data subject can be identified, inter alia, by the following identifiers, mentioned exemplarily in Art. 4(1) GDPR: *"[...]*

- *name,*
- *identification number,*
- *location data,*
- *an online identifier,*
- *or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

As can be derived from Art. 2(1) GDPR and Art. 4(1) GDPR, the actual identification of a natural person is not a requirement for the application of the GDPR, but rather the sheer possibility of identifying said natural personal (Schild, 2021).

3.2 Special categories of personal data

The EU legislator considers that the processing of some categories of personal data, called special categories of personal data or sensitive data, requires more stringent rules than other categories, as the processing of special categories of personal data can potentially endanger the data subject's fundamental rights and freedoms significantly (European Parliament and Council, 2016). Art. 9(1) GDPR concretises the scope of what is to be considered a special category by stating the following: *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."* The categories exhaustively mentioned in Art. 9(1) GDPR can be divided into two parts (Schneider, 2017):

(1) The processing of personal data is prohibited, if the processing of said data could potentially reveal the natural person's *"[...] racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership [...]"*. Art. 9(1) GDPR captures thereby any data which is able to – with a certain degree of probability – produce correct information related to one or more of the categories mentioned and not only data that directly reveals information related to one or more of said categories (Schiff, 2018). The restriction that the data must have the ability to reveal sensitive data correctly with a sufficient probability is necessary since otherwise, the scope of Art. 9(1) GDPR would be considered as too extensive (Matejek & Mäusezahl, 2019; Schiff, 2018).

(2) The second part of Art. 9(1) GDPR covers data that shall not be processed (Schneider, 2017). This data includes *"[...] the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation [...]"*. The meaning of the different wording in parts one and two of Art. 9(1) GDPR can best be demonstrated with an example: location data per se, as mentioned by Schiff (2018), is not mentioned in Art. 9(1) GDPR as a special category of personal data, despite its huge potential to reveal sensitive data. However, by the interpretation of the first part of Art. 9(1) GDPR, location data could also be considered sensitive data if it has the ability to correctly reveal any sensitive information as enumerated under Art. 9(1) GDPR. This example illustrates the importance of the division of Art. 9(1) GDPR and its broad scope, especially due to the first part.

In the case of fitness trackers, the collection of data often concerns health data, which according to Art. 9(1) GDPR is considered sensitive data

(Tzanou, 2020). Therefore, the term health data will be analysed more closely.

Art. 4(15) GDPR defines health data as *"[...] personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"*. Recital 35 GDPR substantiates the meaning of health data even further. Petri (2019) states that the collection of other data not directly related to the health status of a data subject can lead to inferences about the data subject's health. This is especially the case if the data is connected to other information. Data with no direct link to the health status of a data subject is to be considered health data if the data has the ability to correctly derive information about the health status of a data subject with a certain degree of probability (Petri, 2019). Said data is considered health data even in cases where the data controller does not have the intention to process the data in a sense to derive information about the health status of a data subject nor to use the information about the health status of an individual generated from the data (Petri, 2019).

3.3 Data processing

Another important term in the context of Art. 2(1) GDPR is processing. Again, the EU legislator provides a legal definition under Art. 4(2) GDPR, stating, analogously, that processing describes any kind of performance on personal data, such as collection, recording, storage, etc. (European Parliament and Council, 2016). In the context of processing, the GDPR differentiates between the terms 'controller' and 'processor'. According to Art. 4(7) GDPR, *"'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data [...]"*. The processor is defined under Art. 4(8) GDPR as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*. According to these definitions, the GDPR is not only applicable to the institution or entity executing the processing activities but also to the entity that commissions the execution of processing activities (European Commission, n.d.). Summarized, the GDPR distinguishes three entities: data subjects, data controllers and data processors, whereby different rights and obligations, depending on the entity status, are applied (EDPB, 2019).

3.4 Means of data processing

Unfortunately, unlike for other key terms, a concrete definition for the processing by automated means cannot be found in the GDPR (Finck, 2019). However, Herbst (2020a) constitutes that automated processing requires the deployment of any technical tools. Furthermore, Herbst (2020a) refers to the definition of automated processing by the German legislator, enacted in § 3 Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG), marking the deployment of data processing systems as a criterion for automated data processing. While wholly automated processing describes the processing of data without the use of intermediate steps that are executed by persons, partly automated processes are dependent on some kind of human assistance (Ernst, 2021).

The GDPR does not contain a specific legal definition for the processing of personal data other than by automated means. Schuster and Dalby (2019) argue that processing other than by automated means refers to processing that is solely executed by persons, whereby computers are not used in the process. According to Voigt and von dem Busche (2018), the EU legislator assesses the need for protection of personal data by processing other than by automated means lower than by automated means, as the amount of personal data that can be collected is generally significantly lower than by automated means. Therefore, the application of the GDPR in the case of data processing other than by automated means is subject to the condition that the data is either in a filing system or, as stated in Art. 2(1) GDPR, *"[...] intended to form part of a filing system"* (Voigt & von dem Busche, 2018). Based on the criteria set forth by the GDPR, human assistance can be regarded as the demarcation line between wholly or partly automated processes, while the deployment of computers separates automated processing from non-automated processing (Schuster & Dalby, 2019). The reason for extending the application of the GDPR also to non-automated data processing is the aim of the GDPR to be technologically neutral and to prevent circumvention of the application of the GDPR (Schuster & Dalby, 2019).

4 Lawfulness of processing

According to the GDPR, the processing of personal data, where the GDPR is applicable, is generally considered unlawful. Art. 6(1) GDPR presents a list of six specific exceptions that allow for the processing of personal data. This means, for data processing to be lawful, at least one of the conditions set forth in Art. 6(1) GDPR have to be met (European Parliament and Council, 2016). For the processing of special categories of personal data, Art. 9(2) GDPR enumerates ten legal grounds under which processing of said data is considered lawful. Since in the case of wearables, more concretely fitness trackers, the processing of personal data will usually be based on consent, in the case of this bachelor thesis, Art. 6(1)(a) GDPR is considered of higher relevance than other legal grounds for personal data processing (Krishnamurthy, 2020). Furthermore, data collected by fitness trackers is often regarded as a special category of personal data, namely health data, which is subject to even more stringent rules under Art. 9 GDPR (Tzanou, 2020). Therefore, both consent under Art. 6 and Art. 9 GDPR will be elaborated on more extensively in the following sections.

4.1 Definition of consent

The processing of personal data pertaining to a data subject based on the consent of said data subject is regulated under Art. 6(1)(a) GDPR, stating the following: *"Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes [...]"*. According to the EU legislator concerning data processing based on Art. 6(1)(a) GDPR, each person should have the possibility to determine autonomously whether they want to share personal data and if so, be able to decide what kind of personal data they want to share (Buchner & Petri, 2020). Further specifications and clarifications regarding consent are provided in several different articles of the GDPR, mainly Art. 4(11), Art. 6(1)(a), Art. 7, Art. 8, Art. 9, Art. 13, Art. 14 and Art. 22, as well as the accompanying recitals, especially Recitals 32, 33, 42, 43 GDPR (EDPB, 2020).

Consent is explicitly defined under Art. 4(11) GDPR. The text sets forth several requirements that need to be fulfilled for consent to be valid.

According to Art. 4(11) GDPR, consent has to be: ″

- *freely given,*
- *specific,*
- *informed and*
- *an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her″*

In the following sections, each of the requirements will be analysed in more detail.

4.2 Freely given

Recital 43 GDPR specifies the term freely given consent. It states that consent should be regarded as invalid in cases of *″[...] a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation″*. While Recital 43 GDPR explicitly mentions the potential imbalance between public authorities and data subjects, the European Data Protection Board (EDPB) clarified that further constellations of imbalance are possible, e.g. the potential imbalance between employers and employees (EDPB, 2020). However, a potential imbalance between the data controller and data subject shall not per se lead to the invalidity of consent. Recital 43 GDPR clearly states that the validity of consent, even in the case of imbalance of power, depends on the specific situation and should be considered on a case-to-case level (Kühling & Buchner, 2020).

A further indicator of whether consent is freely given can be found in Art. 7(4) GDPR. Consent is regarded to not be freely given if *″[...] the performance of a contract [...] is conditional on consent to the processing of personal data that is not necessary for the performance of that contract″*. The term necessary is to be interpreted strictly (Golland, 2018). For example, the provision of personal data to a social media provider for marketing purposes in exchange for the use of its service is not considered necessary to perform the contract under Art. 7(4) GDPR, even if such a clause is part of the contract. Viewed objectively, the processing of personal data to offer personalised ads is not the core characteristic of a social media platform but rather the provision

of a platform, where people can interact with each other (Golland, 2018). By falsely interpreting this constellation as necessary to perform a contract, the purpose of Art. 7(4) GDPR and the intention of the EU legislators would be circumvented (Golland, 2018). However, legal scholars also argue that such agreements – personal data for service – are regarded as legitimate if agreed upon contractually and in consideration of the transparency requirements under, inter alia, Art. 12 GDPR. Furthermore, the provision of the service must not be advertised as a free service in such cases and importantly, an alternative to consent for the processing of personal data in exchange for the service must be provided, e.g. a monetary exchange for access to the service (Schulz, 2018; Ingold, 2018; Krohm & Müller-Peltzer, 2017). This means that Art. 7(4) GDPR is not to be considered violated if an alternative that does not require consent to the processing of personal data for the provision of the service is available, even if the services are not identical (Ingold, 2018). The EDPB clarifies that the alternative service has to be provided by the same data controller in order to comply with the GDPR (EDPB, 2020).

Another criterion for the determination of whether consent was given freely is granularity. Recital 43 GDPR refers to a situation where the data controller *"[...] does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case [...]"*. Closely related, Recital 32 GDPR further states, inter alia, the following: *"[...] When the processing has multiple purposes, consent should be given for all of them [...]"*. The EDPB considers the lack of choice for which purposes a data subject wants to share their personal data as a restriction in its self-determination and therefore in violation of founding principles of the GDPR, namely Art. 1 GDPR, which emphasises the *"[...] right to the protection of personal data"* (EDPB, 2020).

Detriments resulting from the rejection of consent to data processing is considered a further criterion for assessing whether consent was given freely, which is elaborated in Recital 42 GDPR. The EDPB mentions in its guidelines on consent an example whereby any arising costs from the withdrawal of consent are to be regarded as a detriment (EDPB, 2020). However, Schulz (2018) argues that only grave disadvantages fall under the scope of detriment, albeit without providing a more specific elaboration on what is to be considered a grave disadvantage. As argued by Golland (2018), offering a service, where the data subjects can pay with their personal data and alternatively offering the same service, where payment is executed in the form of money, is regularly considered as a valid alternative without detriment for the data

subject. However, in this case, difficulties arise when trying to exchange the value of personal data into monetary value, even though some concepts have been suggested (Golland, 2018).

4.3 Specific

Art. 5(1)(b) GDPR imposes that personal data can only be processed lawfully *"[...] for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes [...]"*. This article serves as a safeguard to the original idea of the GDPR, namely to give data subjects auto-determination over their personal data by limiting the processing activities of data controllers to a previously agreed extent (Herbst, 2020b). Whether a purpose is described specifically enough cannot be answered in a general manner. The Article 29 Data Protection Working Party (WP 29), the predecessor of the EDPB, clarified in its guidelines on purpose limitation that a purpose is specific when the data subject knows the extent of the processing activities, i.e. which processing activities are undertaken, and the goal of the purpose (WP 29, 2013). In order to fulfil the requirement of consent to be specific, a separate consent option for each purpose has to be made available. Bundling several purposes and allowing data subjects either to consent to all of the purposes or otherwise denying the service to the data subject is neither considered freely given nor specific (EDPB, 2020).

4.4 Informed

Consent can only be regarded as freely given and specific if the information on the types of personal data processed and the reasons for personal data processing are provided (EDPB, 2020). Therefore, information is highly valued in the context of the GDPR and indispensable in order to comply with the main idea of the GDPR, namely, enabling data subjects to determine the degree of data sharing autonomously (Herbst, 2020b). This principle is further embedded in Recital 39 GDPR, arguing that every natural person should know when their personal data is *"[...] collected, used, consulted or otherwise processed [...]"* (Reimer, 2018). A non-exhaustive list of information that has to be provided to each data subject in order to consider them sufficiently informed cannot be found in the GDPR. The requirements for information are rather composed based on several articles and recitals in the GDPR, inter alia, Art. 7, 12, 13, 14, 22 and 46 GDPR, as well as Recital 42 GDPR (EDPB, 2020; Schulz, 2018; Stemmer, 2021).

A list of information provision requirements for the data controller where information is collected from the data subject can be found under Art. 13(1) GDPR, including the requirement to express, inter alia, the following: *"[...] (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; [...] (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; [...]"*. Art. 13(2) GDPR includes further information that has to be provided by the data controller to the data subject before the processing of personal data, for instance, information on the duration of data storage, the right to request the erasure of personal data, the right to withdraw consent, etc.

Art. 14 GDPR provides a similar list of information provision requirements. However, Art. 14 GDPR regulates the circumstances, *"[w]here personal data have not been obtained from the data subject [...]"*. The EDPB stipulates further that data subjects must be informed about the processed data type. However, the EDPB also remarks that the degree of information provided to data subjects is dependent on the specific situation of data processing. Hence, there is no general answer to the required amount of information to give informed consent (EDPB, 2020).

While the above-mentioned information requirements describe concrete examples of information that has to be provided, Art. 12(1) GDPR specifies how the necessary information is to be portrayed, namely *"[...] in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]"*. The idea behind said article is to avoid both a lack of information for the data subject, hence leading to the inability of a data subject to make an informed decision, and an overwhelming provision of information, resulting in a practical impossibility to comprehend the information required to make an informed decision (Greve, 2018). However, Art. 12(1) GDPR does not apply to the provision of any information but, as mentioned in said article, is only applicable for the information requirements alluded to Art. 13 and Art. 14 GDPR and communication requirements mentioned in Art. 15-22 and Art. 34 GDPR. The term intelligible is not defined legally in the GDPR. However, deriving from previous judgements by the European Court of Justice (ECJ), intelligibility is to be interpreted from the stance of a reasonably well-informed average consumer (ECJ, 1998). Art. 12 GDPR is viewed critically in legal literature, as it requires information to be made available in a concise and, at the same time, intelligible form (Dix, 2019; Bäcker, 2020). However, legal scholars emphasise that compliance with Art. 12(1) GDPR

is possible, for example by using a 'multi-layered notice', whereby each layer contains more detailed information (Greve, 2018; Paal & Hennemann, 2021).

Additionally, the WP 29 states, based on the case *Pfeiffer and Others v Deutsches Rotes Kreuz*, that information must be provided to individuals in a direct manner to be regarded as easily accessible (WP 29, 2011). This means it is not considered sufficient to refer to necessary information not available directly to the data subject (WP 29, 2011). For instance, if printed media referred to a website in order to obtain further information on the processing of personal data, the information would not be regarded as easily accessible according to Art. 12(1) GDPR, if said article was to be considered in isolation and interpreted conservatively since the necessary information can no longer be directly accessed (Datenschutzkonferenz, 2018). However, the EU legislator has also foreseen situations in which the provision of information via other tools might be inevitable, namely by introducing Recital 58 GDPR, enabling to provide necessary information via a website (Schulz, 2018). In the concrete case of fitness trackers, where the display size may impede the provision of information in the manner foreseen by Art. 12(1) GDPR, Franck (2018b) argues, in accordance with the WP 29, that the provision of information via another modality (e.g., a website) is the only possible solution.

4.5 Unambiguous agreement to personal data processing

Another element of the GDPR concerns the unambiguousness and clear affirmation of the data subjects' consent to the processing of personal data. Recital 32 GDPR substantiates the meaning of a clear affirmative action with the provision of several examples, inter alia, a written or oral statement, or any *"[...] conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data"*, such as the ticking of a box in the case of electronic media. The EU legislator specifically points out in Recital 32 GDPR that *"[s]ilence, pre-ticked boxes or inactivity should not [...] constitute consent"*, clearly envisaging the prevention of the deployment of 'opt-out methods' by data controllers (Albers & Veit, 2020). Opt-out describes the situation in which consent is already set by default by the data controller. The lack of concrete active conduct to accept the processing of personal data by the data subject in these scenarios leads to the invalidity of consent (Schantz, 2017). The ECJ has also confirmed the clear rejection of opt-out methods in C-673/17, which states that in situations where consent is already set by default by the data controller and the data subject actually has to by an active action refuse consent to the processing

of personal data, is not regarded valid under the GDPR (ECJ, 2019).

4.6 Explicit consent

As previously noted, Art. 9(1) GDPR declares that the processing of sensitive data is prohibited. However, Art. 9(2) GDPR provides certain exceptions that allow the processing of sensitive data. While all the exceptions to the prohibition of personal data processing are enumerated exhaustively under Art. 9(2) GDPR, for the scope of this bachelor thesis, only Art. 9(2)(a) GDPR will be analysed in more detail. Many fitness trackers conduct sensitive data processing based on explicit consent (Krishnamurthy, 2020). Thus, we limited our research to the analysis of Art. 9(2)(a) GDPR, however, we acknowledge that sensitive data might be processed based on other legal grounds.

Art. 9(2)(a) GDPR states that processing of sensitive data is considered lawful if *"the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject"*. Explicitness, as envisaged in Art. 9(2)(a) GDPR, represents a clear demarcation line from normal consent described in Art. 6(1)(a) GDPR. As previously discussed, consent in terms of Art. 6(1)(a) GDPR can be, as described in Recital 32 GDPR, given in a written or oral statement, or in "*[...] any other conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data"*. While a written or oral statement apparently states the data subject's consent to data processing, the last part can be viewed as a conclusive, implicit action by the data subject, which under consideration of all aspects of a specific case, suggests that the data subject's action is a clear indication of their consent to data processing (Ernst, 2017). In the case of sensitive data processing and the more rigorous rules applied to explicit consent under Art. 9(2)(a) GDPR, such conclusive implicit action by the data subject to articulate their consent to the processing of sensitive data is not regarded sufficient (Petri, 2019). The EDPB (2020) suggests in its guidelines on consent that making sure the requirement of explicit consent is fulfilled can be achieved via signed written or oral statements. However, the EDPB also acknowledges that obtaining consent via a written, signed statement is not feasible in many cases. In an example, the EDPB mentions the provision of 'explicit consent screens' which include information on the data processed and where data subjects have the possibility to expressively state their consent via clicking a button that, e.g., says *"I, hereby, consent to*

the processing of my data" as one possibility to obtain explicit consent. The EDPB also makes clear in the same example that the wording of requesting consent is crucial, as, e.g., clicking a button providing the sentence: *"It is clear to me that my data will be processed"*, is not considered as explicit consent (EDPB, 2019).

5 Current data collection and processing

The previous chapters were dedicated to the analysis of the legal text of the GDPR with a specific focus on the material scope and the legal grounds for the processing of personal data. In this chapter, we aim to analyse whether and how privacy policies of companies operating in the field of fitness trackers may have been influenced by the requirements regarding the material scope and the legal grounds for the processing of personal data set forth in the GDPR. In particular, we want to analyse whether privacy policies from European companies have adopted more to the legal requirements and the terminology of the GDPR than companies outside of Europe based on a collective case study. For our analysis, we included six privacy policies from six different companies operating in the field of fitness trackers. In order to examine potential differences in the privacy policies of European companies compared to companies from other continents, we included two European companies, FitTrackerEU1 and FitTrackerEU2, two American companies, FitTrackerUSA1 and FitTrackerUSA2, and two Asian companies, FitTrackerAsia1 and FitTrackerAsia2. The concrete process of how the companies were selected is described in Chapter 2.

For the analysis we derived five factors based on the theoretical review of the GDPR in Chapters 3 and 4 in order to ascertain whether the GDPR may have influenced privacy policies. In Chapter 3, we looked into, inter alia, Art. 4(1) GDPR, which is concerned with the types of data generally considered personal data and Art. 9(1) GDPR, which specifies the types of special categories of personal data. Furthermore, the term processing of personal data and the purposes of personal data processing were reviewed based on the interpretations provided by legal scholars. Thereupon, we derived the first three factors which will be included in the analysis of the privacy policies:

- Are the types of personal data processing mentioned and elaborated in the privacy policies?
- Is the processing of special categories of personal data specifically mentioned in the privacy policies?
- Are the purposes for the processing of personal data mentioned?

The legal grounds for the processing of personal data set forth by the GDPR were discussed in Chapter 4. We specifically focused on consent as a legal ground for the processing of personal data and on explicit consent for the processing of special categories of personal data.

Based thereupon, we derived the fourth factor:

- Is 'consent' and/or 'explicit consent' as a legal basis for personal data processing elaborated?

Lastly, we want to analyse if companies adopted the terminology set forth in the GDPR in their privacy policies. Therefore, we introduced one more factor which enables us to consider this aspect in our analysis, namely:

- Is the terminology set forth in the GDPR mirrored in the privacy policies?

For our analysis, we will consider each factor separately in order to determine to which extent the factors are incorporated into the analysed privacy policies.

5.1 Types of personal data processing

In a first step, the privacy policies were analysed in order to ascertain whether users are informed about the types of personal data processed in the course of the usage of the companies' products and services. The analysis is based on Art. 4(1) GDPR and Art. 9(1) GDPR which provide several examples of types of personal data, such as location data and physical data, described in more detail in Chapter 3. For our analysis, we considered whether companies included types of personal data that are processed in the privacy policies and whether these types were explained in order to make them easier to understand for users. Furthermore, we investigated whether concrete examples of personal data processing activities were included. The results of our analysis for the factor *types of personal data processing* can be seen in Table 1.

While FitTrackerEU2, FitTrackerUSA1 and FitTrackerUSA2 provided an extensive, structured list of the types of personal data processed and additionally included concrete examples of data processing, FitTrackerEU1 failed to provide the necessary information in such format. In the case of FitTrackerEU1, the privacy policy only stated a general clause that personal data is collected when buying or using their products and services. However, a reference to the type of personal data which might be potentially processed cannot be found.

Despite FitTrackerAsia2 mentioning some types of personal data, the privacy policy does not include key elements of data collection, such as health data. An analysis of the fitness trackers' functionalities, however, demonstrates the ability of the fitness tracker to monitor the users' heart rate, which

Table 1: Inclusion of and elaboration on types of personal data, and provision of concrete examples

	FitTrackerEU1	*FitTrackerEU2*	*FitTrackerUSA1*	*FitTrackerUSA2*	*FitTrackerAsia1*	*FitTrackerAsia2*
Types	—	✓	✓	✓	—	∼
Elaboration	—	✓	✓	✓	—	—
Examples	✓	✓	✓	✓	✓	✓

is generally considered health data in the sense of the GDPR (European Parliament and Council, 2016). A fragmentary and incomplete description of the types of data collected leaves users with an incorrect perception of the disclosure of their personal data (Waldman, 2018).

FitTrackerAsia1 provided a comprehensive list of examples of data that is collected. However, the company failed to divide the personal data collected into different types.

5.2 Special categories of personal data

This section is concerned with the processing of special categories of personal data and whether the privacy policies analysed indicate that such processing activities are conducted. Based on the observations stipulated in Chapter 3, the EU legislator envisages more stringent regulations when processing sensitive data. All fitness trackers analysed for this thesis share one functionality: monitoring the users' heart rate, which is generally considered sensitive data (European Parliament and Council, 2016). Therefore, we analysed if the companies mention in their privacy policies that special categories of personal data are processed. The results for the factor *mentioning that special categories of personal data are processed* can be seen in Table 2.

In our research, we discovered that the processing of special categories of personal data is not mentioned in the privacy policies provided by FitTrackerUSA2 and FitTrackerAsia2.

FitTrackerAsia1 states in its privacy policy in one section of its privacy policy that it does not collect sensitive personal data. However, contrary to this assertion, the company clearly points out in another section of the respective privacy policy that sensitive personal data, such as heart rate data, is processed.

Table 2: Mentioning that special categories of personal data are processed

	FitTrackerEU1	FitTrackerEU2	FitTrackerUSA1	FitTrackerUSA2	FitTrackerAsia1	FitTrackerAsia2
Processing of sensitive data mentioned	~	✓	~	—	~	—

FitTrackerEU1's and FitTrackerUSA1's privacy policies mentioned that sensitive data might be processed. However, instead of explaining concretely which part of the data collected is to be regarded as sensitive data, only a very broad and general note that sensitive data might be collected is provided.

Only FitTrackerEU2 describes in its privacy policy the types of sensitive personal data collected, and additionally provides concrete examples of sensitive data processing.

5.3 Purposes for data processing

In this section, we analysed whether the privacy policies elaborate on the reasons for which the personal data has been processed, since according to Art. 5(1)(b) GDPR, data may only be processed for specific purposes. The concrete requirements for the processing of personal data are described in more detail in Chapter 3. We analysed whether the purposes for which personal data processing is conducted are generally mentioned and, if so, whether additional information, such as concrete examples, is provided. The results for the factor *inclusion of purposes for personal data processing* can be seen in Table 3.

Generally, the companies show a similar approach towards the inclusion and description of the purposes for data processing in their privacy policies. The most common purposes identified are: (i) improvement of the product and service; (ii) marketing; and (iii) personalisation of service and product.

All companies, except FitTrackerEU1, describe the purposes for which data is processed in a separate section of the privacy policy. FitTrackerEU2 and FitTrackerUSA1 follow an organised structure in the description of the purposes. The section is divided into several subsections, whereby each subsection represents one purpose. Each purpose is elaborated in detail and additionally includes examples. Only FitTrackerEU1 fails to provide a dedicated section concerned with an elaboration on the purposes for which data is processed. The term purpose can be found 21 times in the privacy policy;

Table 3: Mentioning and explaining the purposes of personal data processing

	FitTrackerEU1	*FitTrackerEU2*	*FitTrackerUSA1*	*FitTrackerUSA2*	*FitTrackerAsia1*	*FitTrackerAsia2*
Purposes mentioned	✓	✓	✓	✓	✓	✓
Purposes elaborated	–	✓	✓	✓	✓	✓

however, the company does not provide the purposes of data processing in a clear, transparent and compact manner. Users are forced to cumbersomely navigate through different parts of the privacy policy in order to find the purposes for which their data is processed.

5.4 Lawfulness of processing

Art. 6(1) GDPR and Art. 9(2) GDPR enumerate an exhaustive list of legal grounds under which the processing of personal data, respectively the processing of special categories of personal data, is considered legal. As elaborated in more detail in Chapter 4, Art. 6(1)(a) GDPR and Art. 9(2)(a) GDPR stipulate (explicit) consent by the data subject as one possible legal basis for the processing of (special categories) of personal data. In our practical evaluation of the online privacy policies, we analysed whether (explicit) consent as a legal ground for the processing of personal data is mentioned. More concretely, we wanted to ascertain whether the online privacy policies elaborated on the requirements set forth in the GDPR for consent, according to Art. 6(1)(a) GDPR, and explicit consent, according to Art. 9(2)(a) GDPR. The results for the factor *elaboration on (explicit) consent as a legal ground for personal data processing* can be seen in Table 4.

All privacy policies mentioned consent as one possible legal basis for the processing of personal data. However, only FitTrackerEU1 and FitTrackerEU2 explained in their privacy policy how consent might be obtained from the data subject. FitTrackerUSA1, FitTrackerUSA2, FitTrackerAsia1 and FitTrackerAsia2 did not provide any additional information regarding the method used to obtain consent from the data subjects.

Furthermore, we found that only two companies, namely FitTrackerEU2 and FitTrackerUSA1, included consent and explicit consent as two separate terms, while none of the other companies mentioned explicit consent. FitTrackerEU2 merely mentioned that explicit consent is required for the

Table 4: Inclusion of and elaboration on consent and explicit consent as legal bases for the processing of personal data

	FitTrackerEU1	*FitTrackerEU2*	*FitTrackerUSA1*	*FitTrackerUSA2*	*FitTrackerAsia1*	*FitTrackerAsia2*
Consent mentioned	✓	✓	✓	✓	✓	✓
Consent elaboration	✓	✓	–	–	–	–
Explicit consent mentioned	–	✓	✓	–	–	–
Explicit consent elaboration	–	–	✓	–	–	–

processing of sensitive personal data, however, did not elaborate on what the difference between consent and explicit consent is. FitTrackerUSA1 provided more information on what is meant by the term explicit consent and how such explicit consent is obtained.

5.5 Terminology of privacy policies

This section is dedicated to the analysis of the language of the privacy policies. Concretely, the aim was to assess whether the terminology used in the GDPR is mirrored in the privacy policies. For the assessment of the terminology of the privacy policies, we analysed whether the following terms provided in the GDPR were also used in the privacy policies:

- personal data
- types of personal data processing, namely location, physical, physiological and health data;
- special categories of personal data or sensitive data;
- purposes;
- consent and explicit consent as legal grounds for the processing of personal data.

The limitation to location, physical, physiological and health data in the case of analysing the types of personal data stems from the focus on fitness trackers and their functionality of measuring location, physical, physiological and health data. However, even though we acknowledge that other types of

Table 5: Inclusion of terms specified in the GDPR

	FitTrackerEU1	*FitTrackerEU2*	*FitTrackerUSA1*	*FitTrackerUSA2*	*FitTrackerAsia1*	*FitTrackerAsia2*
personal data	✓	✓	✓	✓	✓	✓
location data	✓	✓	✓	✓	✓	✓
physical data	—	—	✓	—	—	—
physiological data	—	—	—	—	—	—
health data	—	✓	✓	✓	—	—
sensitive data	✓	✓	✓	—	✓	—
purposes	✓	✓	✓	✓	✓	✓
consent	✓	✓	✓	✓	✓	✓
explicit consent	—	✓	✓	—	—	—

data may be derived from the types of data considered for our analysis, such as *"[...] political opinions, religious or philosophical beliefs, or trade union membership [...]"* mentioned in Art. 9(1) GDPR, we explicitly do not include these in our analysis, as the inclusion and consideration of all possible types of personal data is beyond the scope of this thesis. Table 5 illustrates the results for the factor *terminology of privacy policies*.

All companies included the terms personal data, location data, purpose and consent according to the terminology in the GDPR. Only FitTrackerUSA1 pointed out in its privacy policy that physical data is processed, while none of the other privacy policies referred to physical data explicitly. Furthermore, the term physiological data is not included in any of the analysed privacy policies, despite the fact that fitness trackers collect physiological data, such as heart rate data (Lin et al., 2005). While the term physiological data was not included in any of the privacy policies, some companies, namely FitTrackerEU2, FitTrackerUSA1 and FitTrackerUSA2, labelled physiological data, such as the user's heart rate, as health data.

While Art. 9(1) GDPR refers to special categories of personal data, only FitTrackerEU2 and FitTrackerUSA1 adopted this term. FitTrackerEU1 and FitTrackerAsia1 used the term sensitive data to describe the processing of special categories of personal data, a term, which can be found in, inter alia, Recital 51 GDPR. FitTrackerUSA2 and FitTrackerAsia2 generally did not

consider special categories of personal data.

All companies described the reasons for which data processing is conducted with the term *purpose*, identical to the term mentioned in the GDPR.

Only FitTrackerEU2 and FitTrackerUSA1 mentioned explicit consent as a legal basis for the processing of sensitive data, while none of the other companies elaborated on which legal grounds sensitive data is processed.

6 Proposal of framework

In this chapter, we present the PPAF, a framework that enables users to individually assess how privacy policies may have been influenced by the GDPR's material scope and legal grounds for personal data processing. Based on our literature review on the GDPR's material scope and the legal grounds for personal data processing in Chapters 3 and 4 and our subsequent analysis of privacy policies in Chapter 5, the PPAF particularly focuses on three aspects, namely examining the design, information and the understandability of privacy policies, as displayed in Figure 2.

Design. Firstly, the design of the analysed privacy policy is considered. This aspect stems from our analysis of how information should be presented in Chapter 4. According to Art. 12(1) GDPR information has to be provided in an, inter alia, *"[...] easily accessible form [...]"*. Furthermore, Recital 60 GDPR states that information regarding personal data processing *"[...] may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing"*. Based thereupon, this aspect is mainly concerned with the comfortability of finding the required privacy policy and how the privacy policy is displayed.

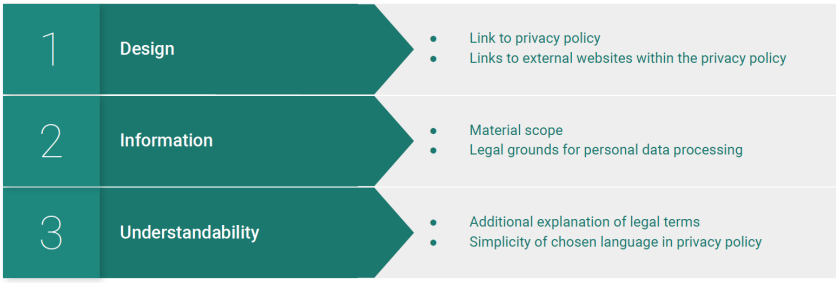
Information. The second aspect is concerned with whether privacy policies include information on the material scope and the legal grounds for personal data processing according to the GDPR. This aspect of our proposed framework stems from our literature review concerning the legal interpretation of the GDPR's material scope and the legal grounds for personal data processing in Chapters 3 and 4, and our analysis of privacy policies in Chapter 5. The aspect information follows a two-fold approach:

(1) In the first step, we suggest analysing whether the information is provided mirroring the terminology set forth in the GDPR.

(2) The second step becomes relevant if the analysed privacy policy does not use GDPR terminology. In this case, we propose analysing whether the information is provided in privacy policies by using other terms than those set forth in the GDPR.

Understandability. The last aspect is concerned with the evaluation of the understandability of privacy policies. As discussed in Chapter 4, Art. 12(1) GDPR states that information has to be provided *"[...] using clear and plain language [...]"*. Therefore, this aspect specifically refers to the use of legal

Figure 2: Overview of the aspects considered in our proposed framework



terms and the potential lack of transparent and straightforward explanations of said terms in the analysed privacy policies.

Each of the considered aspects supports the framework's users to determine whether the privacy policy may have been impacted by the respective requirements mentioned in the GDPR. Potential users of the PPAF are, for example:

Researchers and legal scholars. The PPAF can be used by researchers and legal scholars operating in the field of the GDPR. Based on our literature review in Chapters 3 and 4 and our subsequent analysis of privacy policies in Chapter 5, we identified several parameters which support researchers and legal scholars to systemically determine whether the analysed privacy policies include information which relates to the GDPR's material scope and the legal grounds for personal data processing. Due to our focus on fitness trackers, our framework also specifically includes parameters related to special categories of personal data and explicit consent. Furthermore, we identified concrete terms commonly used in privacy policies when referring to the GDPR's material scope and legal grounds for personal data processing which are not mentioned in the GDPR. Based on our findings, researchers and legal scholars can use the PPAF as a starting point to create a corpus of relevant terms mentioned in privacy policies relating to the GDPR's material scope and legal grounds for personal data processing. For example, the output can be used as the basis for the development of automated privacy policy analysis tools.

Furthermore, our procedure on incorporating the GDPR's material scope and legal grounds for personal data processing into the PPAF can be used as a guideline for the addition of other aspects related to the GDPR, such as the territorial scope.

Data subjects. Several studies and surveys show that privacy policies are

generally considered difficult to read and understand by data subjects due to lengthy and complicated texts (Reidenberg et al., 2014; Litman-Navarro, 2019; Morel & Pardo, 2020). Our proposed framework supports data subjects by providing guidance on how to read privacy policies. The PPAF informs users about privacy requirements set out in the GDPR and includes concrete examples of terms related to these requirements. Data subjects can, e.g., check whether these terms are mentioned in privacy policies and determine how the respective data controller intends to use their personal data. However, we acknowledge that the use of the framework for this user group might be limited. A study conducted by McDonald and Cranor (2008) shows that if an average internet user wanted to read all the privacy policies of the websites they visited in a year, it would take them approximately 250 hours. While the PPAF might increase the understandability of privacy policies, it would require a considerable effort to read all privacy policies and analyse them using our framework.

Companies. Another group that could benefit from our proposed framework are companies. Companies can use the PPAF in order to check whether their privacy policy follows the structure set forth by the GDPR. Furthermore, companies can align the terminology used in their privacy policies to the GDPR's terminology based on the information provided in our framework. However, although the PPAF allows determining whether privacy policies follow the GDPR's structure and terminology, it does not provide any information on whether privacy policies comply with the requirements described in the GDPR. In order to derive a conclusion on whether a company's privacy policy is GDPR-compliant, a multitude of different aspects need to be considered and analysed on a case by case level. While including the information according to the proposed PPAF might increase the informative value of the privacy policies, it does not automatically lead to compliance with the regulations described in the GDPR.

Developers. Further potential users of our proposed framework are developers of privacy policies. While companies are a potential sub-group of privacy policy developers, other stakeholders need to develop privacy policies under certain circumstances as well. For example, privacy policies might be necessary in the case of a research project in order to inform research participants about potential data processing activities (Sheffield Hallam University, n.d.). Moreover, public institutions, such as universities, need to publish privacy policies under certain circumstances (Vienna University of Economics and Business, 2019). The PPAF can be considered a guideline for creating privacy policies, particularly for the parts concerning the GDPR's material scope and legal grounds for personal data processing.

As discussed in Chapter 2, the framework was generated based on a collective case study research (Crowe et al., 2011). Our theoretical research into the legal text of the GDPR, more specifically the material scope and the legal grounds for personal data processing, enabled a clear understanding of the terms set forth in the GDPR. Based on this understanding, we analysed six different privacy policies, which represent the cases in our research. The criteria for the selection of privacy policies is described in detail in Chapter 2. The analysis of the cases allowed us to define parameters, usually in the form of questions, that can be used to study privacy policies in order to determine whether the respective privacy policy may have been influenced by GDPR's terminology, material scope and the legal grounds for the processing of personal data.

In the following, we present each aspect of the PPAF separately and elaborate on the intended use of the framework. Apendix A shows a compact guidance form of the PPAF's aspects and the relevant parameters for each aspect. It can be found in Appendix A to this thesis.

6.1 Design of privacy policies

Based on the requirements set forth in Art. 12(1) GDPR and Recital 60 GDPR which, inter alia, require a clear presentation and display of information related to personal data processing, we identified two parameters in order to determine how the GDPR may have influenced privacy policies:

- How **easily accessible** are privacy policies?
  We discovered during our analysis that the level of complexity of navigating to privacy policies differed greatly. While, in some cases, the link to a companies' privacy policy was displayed visibly, the design of other websites impeded the discovery of the link to the companies' privacy policy in a straightforward manner. Although companies usually used the term privacy policy for information on personal data processing, we found that this information was often provided under other terms, with the most prominent ones being 'privacy', 'privacy statement' and 'privacy note'.

- How is the **information displayed** in the privacy policies?
  A survey conducted by the European Commission (2019) identified the length and complexity of privacy policies to be the principal reason why privacy policies are not read. The transparent display of relevant information in a compact, easily legible and yet informative manner

is regarded as an important task to privacy policy providers to enable potential users to gather the necessary information straightforwardly on the processing of their personal data (Waldman, 2018). We found differences in the presentation of information in privacy policies. Some websites only occasionally provided links for further, more detailed information on certain aspects, while most of the information could be found in the company's privacy policy. However, other companies distributed the information regarding the processing of personal data through various websites. Furthermore, our research found that some companies highlighted certain passages in privacy policies in the form of a different font, heading or the use of icons. However, other privacy policies applied the same format for the entire document without emphasising certain parts.

6.2 Information

This subchapter is concerned with analysing whether information regarding the GDPR's material scope and the legal grounds for personal data processing are mentioned in the respective privacy policy. The considered factors stem from our literature review in Chapter 3 and 4 as well as the subsequent analysis of privacy policies in Chapter 5.

In a first step, we propose analysing whether the privacy policies mirrored GDPR terminology. Generally, every industry develops its specific terminology tailored to its needs (McGinnis & Rappaport, 2017). This leads to a situation in which two equal words can be defined completely different depending on the industry they are used in. A consistent terminology within a certain industry is therefore considered important in order to facilitate communication and enable a common understanding (van Mil & Henman, 2016; Barnbrook, 2006; Sageder, 2010). While uniform terminology is relevant in many disciplines, it is considered crucial in legal studies since the clear definition of terms reduces the risk of ambiguous interpretations of the respective terms (Busse, 1991). When a clear definition of a term is missing, different readers might understand the term differently. A similar problem arises in the case of synonyms. For example, the term personal data has already been defined in the GDPR, as discussed in Chapter 3. However, in our analysis of privacy policies in Chapter 5, we discovered that some companies expressed personal data as personal information. Such deviations from legally defined terms make it more difficult for readers of privacy policies to identify data as personal data according to the GDPR (Hill et al., 2012). Therefore, overlapping terminology between privacy policies and the legal text in the GDPR is advantageous (Hill et al., 2012).

In case the analysed privacy policy does not mirror the GDPR's terminology, the second step consists of evaluating whether the considered information has generally been provided, potentially using other terms than those foreseen by the GDPR. In our framework, we include, based on our analysis in Chapter 5, examples of terms that are commonly mentioned in privacy policies but cannot be found in the GDPR.

Our research in Chapters 3 and 4 and our analysis of privacy policies in Chapter 5 led to the identification of six parameters in order to determine whether information regarding the GDPR's material scope and legal grounds for personal data processing is provided. For the PPAF, we propose including the following parameters for the assessment of privacy policies:

- Is there a specific reference to **personal data?**
  Art. 4(1) GDPR defines personal data as *"[...] any information relating to an identified or identifiable natural person [...]"*. During our research, we identified that in some cases privacy policies did not use the term personal data when referring to *"[...] information relating to an identified or identifiable natural person [...]"*. We discovered that some companies used the terms personal information and personal data alternately in their privacy policies. Other terms were not found in the privacy policies.

- Are the **types of personal data** processing specifically mentioned according to Art. 4(1) GDPR and Art. 9(1) GDPR?
  Art. 4(1) GDPR and Art. 9(1) GDPR state different types of data which are regarded as personal data, such as *"[...] one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*. Readers of privacy policies are able to identify data as personal data more easily if the information on data processing in the respective privacy policy uses the GDPR's terminology (Hill et al., 2012). Our analysis in Chapter 5 showed that companies rarely followed the structure set forth by the GDPR regarding the types of personal data. Instead, we identified the following types to be commonly mentioned: (i) device information, (ii) usage data, (iii) account information, (iv) payment information, and (v) information from third parties. However, since these types of personal data are not legally defined, each company can interpret these types individually. For example, (iii) account information in some cases includes the account user's height and weight, while in other cases, such information is not considered to fall under the scope of account information. Furthermore, we found that some companies did not mention

any types of personal data but merely provided a list of concrete examples of data that is processed, such as name, e-mail, gender, height, weight, body temperature, etc.

- Is the processing of personal data referred to as **processing of personal data?**
  According to Art. 4(2) GDPR, personal data processing can be regarded as a collective term for different operations on personal data, such as the *"[...] collection, recording, organisation, structuring, storage, adaptation or alteration [...]"* of personal data. In our research, we discovered that the definition and use of the term processing of personal data differed from its original definition stated under Art. 4(2) GDPR. In some cases, the collection of personal data and the processing of personal data were mentioned as two individual terms, while, according to the GDPR, the collection of personal data is, in fact, a part of personal data processing. Therefore, data processing and data collection cannot be viewed as two dissociated, independent terms. We observed similar scenarios with other terms mentioned in Art. 4(2) GDPR, particularly with the terms (i) recording, (ii) use, and (iii) storage of personal data.

- Is the **processing of special categories of personal data** explicitly and separately mentioned?
  Consent to disclose personal data often depends on the types of data that are to be processed. Data that people consider to be more sensitive is revealed less often than types of data that are not regarded as sensitive (Yang & Wang, 2009). Therefore, readers of privacy policies could potentially react differently in their approach towards the processing of their personal data if they were made aware that certain categories of their data are regarded as special for the reasons provided in Art. 9(1) GDPR. In our analysis, we discovered that most companies mentioned either the term special category of personal data or sensitive data. Companies that did not adopt GDPR terminology generally did not provide any information regarding sensitive data.

- Are the reasons for personal data processing defined as **purposes?**
  According to Art. 5(1) GDPR, the processing of personal data has to be limited to its specified purposes. The purposes can be defined as the reasons for personal data processing (Information Commissioner's Office, n.d.). Since the GDPR refers to such reasons as purposes, companies can increase the comprehensibility of their privacy policies by mirroring GDPR terminology (Hill et al., 2012). Furthermore, Hill et

al. (2012) highlight in their research the importance of consistent terminology in order to achieve a uniform understanding of the discussed topic. However, in our research, we discovered that in some cases companies additionally used other terms to describe the reasons for personal data processing. In addition to the term purpose, we identified further three terms that companies mentioned in order to describe why they process personal data: (i) use of personal information, (ii) how we use personal data, (iii) reasons for personal data processing.

- Are the **legal grounds for personal data processing** mentioned in the privacy policy?
  The GDPR states certain exceptions from its general prohibition of personal data processing under, inter alia, Art. 6(1) GDPR and Art. 9(2) GDPR, as discussed in Chapter 4. For privacy policies to be regarded as easily understandable and straightforward, the legal grounds for the processing of personal should be provided using the same terms as mentioned in the GDPR. According to Hill et al. (2012) and their work in the field of strategy research, the understandability of terms is increased if they are applied uniformly. Due to our limitation to consent and explicit consent as legal grounds for personal data processing in Chapter 4, our analysis in Chapter 5 exclusively considered whether consent and explicit consent are mentioned as legal grounds for the processing of personal data in the analysed privacy policies. Our analysis showed that all companies included consent as a legal basis for personal data processing. However, despite all fitness trackers processing special categories of personal data according to their product descriptions, only two companies mentioned explicit consent as a legal basis for the processing of sensitive personal data. In the other cases, explicit consent was not referred to at all.

6.3 Understandability

The last aspect of the proposed PPAF is concerned with the general understandability of privacy policies. For this aspect, we identified one parameter in order to assess if privacy policies may have been impacted by the regulations set forth in the GDPR regarding the understandability of privacy policies:

- Are technical terms explained using **clear and plain language?**
  Privacy policies, by nature, include many legal terms whose definition in some cases differs from their meaning when applied in everyday

language (Busse, 1991). However, despite the necessity of including technical terms in privacy policies, privacy policies can still be written straightforwardly. In fact, Art. 12(1) GDPR states that information regarding personal data processing has to be provided *"[...] in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]"*. The WP 29 (2018) points out several concrete specifications for fulfilling the requirements set forth in Art. 12(1) GDPR. For example, legal terminology and modal verbs should be widely avoided. Nonetheless, if the use of legal and technical terms is necessary, the meaning of these terms should be specifically explained (Franck, 2018a). However, legal scholars note that in practice, it is often difficult to clearly determine whether information is provided according to Art. 12(1) GDPR due to the general wording used and the partly contradictory requirements outlined in Art. 12(1) GDPR (Bäcker, 2020; Quaas, 2021; Dix, 2019; Paal & Hennemann, 2021; Franck, 2018a). (Bäcker, 2020) therefore argues that a breach of Art. 12(1) GDPR is practically challenging to justify.

For readers of privacy policies to be able to self-autonomously determine the level of data they are willing to reveal, understanding the privacy policy can be regarded as a key element (Pollach, 2007). Our analysis in Chapter 5 showed that companies often explained the terms they mentioned in their privacy policies. However, in some cases we observed that companies used legal terms, such as sensitive data, without stating examples for sensitive data.

7 Conclusion

In this bachelor thesis, we aimed to develop a framework that supports its users to easier read and understand privacy policies with a specific focus on the GDPR's material scope and legal grounds for personal data processing. We defined one overarching research question and three sub-questions that helped us determine the framework's concrete structure and content.

The first research sub-question relates to investigating the definition and scope of the GDPR's material scope and legal grounds for personal data processing according to the GDPR. In order to answer the question, we conducted an integrative literature review using primarily legal literature from German-speaking countries. The literature review helped us to identify primarily two terms that are considered relevant regarding the GDPR's material scope, namely personal data and the processing of personal data (Kühling & Raab, 2020). Regarding the GDPR's legal grounds for personal data processing, we limited our scope to consent, as consent is generally considered the main legal basis for companies to process personal data (Krishnamurthy, 2020).

Personal data. Art. 4(1) GDPR defines personal data as *"[...] any information relating to an identified or identifiable natural person ('data subject') [...]"* and includes several examples of types of data that could lead to the identification of a data subject. Furthermore, the EU legislator considers that some data, such as health data, needs additional protection as it endangers the data subject's fundamental rights and freedoms significantly (European Parliament and Council, 2016). These types of data are called special categories of personal data or sensitive data (European Parliament and Council, 2016).

Processing of personal data. The GDPR defines the term processing of personal data under Art. 4(2) GDPR. In summary, the GDPR considers any performance on personal data, such as collection and storage, as processing of personal data.

Consent. According to Art. 4(11) GDPR, consent needs to be *"[...] freely given, specific, informed and [...]"* unambiguously agreed to. In case of sensitive data processing, the EU legislator foresees obtaining explicit consent (European Parliament and Council, 2016). Explicit consent needs to fulfil the same requirements as consent according to Art. 4(11). However, while consent can be obtained by a conclusive, implicit action of the data subject, explicit consent needs to be obtained by an explicit statement (Petri, 2019; EDPB, 2019).

Despite EU legislators including legal definitions in the GDPR, legal

scholars point out that a clear delimitation of the scope of the terms mentioned in the GDPR is difficult (Kühling & Buchner, 2020). Our literature review showed that legal scholars therefore often refer to current jurisprudence, clarifications made by the EDPB on the interpretation of certain terms or other regulations in order to define the scope of the terms mentioned in the GDPR.

In a second step, we wanted to investigate how privacy policies currently disclose information relating to the GDPR's material scope and legal grounds of personal data processing. Thus, we analysed six privacy policies published by companies that offer fitness trackers from Europe, America and Asia based on a collective case study. We found that most companies mentioned some types of personal data. However, privacy policies often do not include information on the processing of sensitive data. While all privacy policies state consent as one legal ground for personal data processing, only two companies additionally mentioned explicit consent. Furthermore, we discovered that companies mostly mirror the terminology used in the GDPR.

With our third research sub-question, we aimed to ascertain the necessary steps in order to develop a framework that supports users in determining whether information relating to the GDPR is included in privacy policies. We discovered that the development of such a framework requires a theoretical discussion on the GDPR's legal requirements based on a literature review. Due to the often difficult delimitation of legal terms used in the GDPR, it is necessary to include several opinions from legal scholars on the interpretation of the legal requirements. The literature review allowed us to gain an understanding of the intended regulation by the EU legislator. However, we considered that a framework could not only root in a theoretical discussion on the GDPR but also requires insights into how privacy policies currently disclose information. Therefore, we discovered that a case study analysis could additionally contribute to developing a framework with concrete examples of current practices.

Based on our integrative literature review and our case study analysis, we were able to propose a framework as intended with our overarching research question. We identified three aspects that enable users of the proposed Privacy Policy Appraisal Framework (PPAF) to determine how privacy policies display information and whether information concerning the GDPR's material scope and legal grounds for personal data processing are mentioned. The first aspect relates to the accessibility and the layout of privacy policies. In

the second aspect, the content of the privacy policy is analysed. We propose six parameters that support the PPAF's users to determine whether information on the material scope and the legal grounds for personal data processing is provided (i) following the terminology set forth in the GDPR, (ii) using other terms than those mentioned in the GDPR or (iii) is missing. The last aspect necessary to determine whether privacy policies include information on the material scope and the legal grounds for personal data processing according to the GDPR refers to the understandability of privacy policies.

Despite gaining insights that allowed us to develop the PPAF, we identified several limitations in our chosen research methods.

The first limitation relates to the scope of our literature review. We limited our literature review to literature from within the EU. Even more, we predominantly focused on comments provided by legal scholars from German-speaking countries. While the GDPR was introduced in the EU by EU legislators, the regulations set forth in the GDPR have a global impact (Uecker, 2019). Therefore, legal scholars and researchers from outside the EU also reviewed the GDPR and composed articles expressing their opinions (Safari, 2017; Meyers, 2019; Ryngaert & Taylor, 2020). We excluded these opinions that might have added additional relevant insights into our literature review during our research.

Another limitation that we identified concerns our analysis of privacy policies. We included six companies from three different continents in order to determine potential differences in disclosing information regarding the GDPR's material scope and legal grounds for personal data processing. However, the number of analysed privacy policies is too small in order to derive potential regional trends and differences regarding the display of information.

Lastly, the PPAF is limited to certain aspects of the GDPR. For example, we only considered consent and explicit consent as legal grounds for personal data processing in our research. Even though companies, in most cases, process personal data based on consent, the GDPR also foresees other legal grounds for the lawful processing of personal data (Krishnamurthy, 2020). Moreover, we excluded several parts of the GDPR, such as the territorial scope or the right to be forgotten, altogether in our research.

Based on the identified limitations, we suggest several adaptions for future research. Firstly, we suggest incorporating legal literature from outside of the EU. Researchers could explore how legal scholars from other continents interpret legal terms set forth in the GDPR. The PPAF could be extended by these insights and thereby become more suitable for use in an international

context.

Secondly, we propose extending our research and including other parts of the GDPR. For instance, other legal bases for personal data processing, the territorial scope, the right to be forgotten, transfers of personal data to third parties, and many other aspects concerning the GDPR could be subject to research and incorporated into our proposed framework.

Finally, our case study analysis should be enhanced by incorporating more privacy policies. Only with the inclusion of more privacy policies potential regional differences in the disclosure of information in privacy policies could be determined. Furthermore, we suggest testing the PPAF on additional privacy policies and adapting it based on the results.

Despite the identified limitations, this thesis yields a framework that supports the framework's users to systematically analyse whether information on the GDPR's material scope and legal grounds for personal data processing is mentioned. The proposed framework helps other researchers to structurally identify information relating to the material scope and the legal grounds of personal data processing. Based thereupon, common terms mentioned in privacy policies can be identified and mapped to terms used in the GDPR. Researchers can use the framework in order to determine how the disclosure of information in privacy policies has changed over the years and with the introduction of new privacy regulations. In addition, the framework can serve as an orientation for companies in order to adapt their privacy policies to the structure and terminology set forth by the GDPR. These non-exhaustive examples of the possible use scenarios of the PPAF show how the framework contributes to existing and future research.

References

Albers, M., & Veit, R.-D. (2020). DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung [Art. 6 GDPR Lawfulness of processing]. In A. Wolff & S. Brink (Eds.), *Bek'sche Online-Kommentare [Beck's online comments]* (37th ed.). C.H. Beck.

Albrecht, J. P. (2019). Einführung zu Artikel 6 [Introduction to Article 6]. In S. Simitis, G. Hornung, & I. Spiecker (Eds.), *Datenschutzrecht. DSGVO mit BDSG [Data protection law. GDPR with BDSG]* (1st ed.). Nomos Verlagsgesellschaft.

Bäcker, M. (2020). DS-GVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person [Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject]. In J. Kühling & M. Buchner (Eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG [General Data Protection Regulation, Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Barnbrook, G. (2006). *Meaningful Texts: The Extraction of Semantic Information from Monolingual and Multilingual Corpora*. Continuum. Retrieved from `https://permalink.obvsg.at/wuw/AC05721833`

Brodin, M. (2019). A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. *European Journal for Security Research*, *4*(2), 243–264. doi: 10.1007/s41125-019-00042-z

Buchner, B., & Petri, T. (2020). DS-GVO Art. 6 Rechtmäßigkeit der Verarbeitung [Art. 6 GDPR Lawfulness of processing]. In J. Kühling & M. Buchner (Eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG [General Data Protection Regulation, Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Busse, D. (1991). Juristische Fachsprache und öffentlicher Sprachgebrauch. Richterliche Bedeutungsdefinitionen und ihr Einfluß auf die Semantik politischer Begriffe [Legal jargon and public usage. Judicial definitions of meaning and their influence on the semantics of political terms]. In F. Liedtke, M. Wengeler, & K. Böke (Eds.), *Begriffe besetzen. Strategien des Sprachgebrauchs in der Politik [Occupying terms. Strategies of language use in politics]* (1st ed.). Westdeutscher Verlag.

Columbia Mailman School of Public Health. (n.d.). *Content Analysis.* Retrieved from `https://www.publichealth.columbia.edu/research/population-health-methods/content-analysis` (Accessed on March 30, 2022)

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*,

1(3), 100. doi: 10.1186/1471-2288-11-100

Datenschutzkonferenz. (2018). *Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung [Paper No. 10 information requirements for third-party and direct collection].* Retrieved from `https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf` (Accessed on December 20, 2021)

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Proceedings 2019 Network and Distributed System Security Symposium.* Internet Society. doi: 10.14722/ndss.2019.23378

Dix, A. (2019). DSGVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person [Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject]. In S. Simitis, G. Hornung, & I. Spiecker (Eds.), *Datenschutzrecht. DSGVO mit BDSG [Data protection law. GDPR with BDSG]* (1st ed.). Nomos Verlagsgesellschaft.

Dorsemaine, B., Gaulier, J.-P., Wary, J.-P., Kheir, N., & Urien, P. (2015). Internet of Things: A Definition & Taxonomy. In *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies.* doi: 10.1109/NGMAST.2015.71

ECJ. (1998). *Gut Springenheide GmbH and Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt - Amt für Lebensmittelüberwachung.* (No. C-210/96).

ECJ. (2019). *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH.* (No. C-673/17).

EDPB. (2019). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).* Retrieved from `https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf` (Accessed on December 20, 2021)

EDPB. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679.* Retrieved from `https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf` (Accessed on December 20, 2021)

Ernst, S. (2017). Die Einwilligung nach der Datenschutzgrundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO [Consent under the General Data Protection Regulation. Notes on the definition according to Art. 4(11) GDPR]. *ZD Zeitschrift für Datenschutz*, *7*(3),

110–114.

Ernst, S. (2021). DS-GVO Art. 2 Sachlicher Anwendungsbereich [Art. 2 GDPR Material scope]. In B. Paal & D. A. Pauly (Eds.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG [General Data Protection Regulation Federal Data Protection Act]* (3rd ed.). C.H. Beck.

European Commission. (n.d.). *What is a data controller or a data processor?* Retrieved from `https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en` (Accessed on December 20, 2021)

European Commission. (2019). *Special Eurobarometer 487a - March 2019. "The General Data Protection Regulation". Summary.* Retrieved from `https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf` (Accessed on February 17, 2022)

European Data Protection Supervisor. (n.d.). *The History of the General Data Protection Regulation.* Retrieved from `https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en` (Accessed on March 08, 2022)

European Parliament. (2016). *Data protection reform - Parliament approves new rules fit for the digital era.* Retrieved from `https://www.europarl.europa.eu/news/en/press-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era` (Accessed on March 08, 2022)

European Parliament and Council. (2016). 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). *OJ*, *L 119*, 1–88.

European Parliament, the Council and the Commission. (2012). CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2012/C 326/02). *OJ*, *55*, 391–407.

Finck, M. (2019). Smart Contracts as a Form of Solely Automated Processing Under the GDPR. *Max Planck Institute for Innovation & Competition Research No. 19-01*. doi: 10.2139/ssrn.3311370

Franck, L. (2018a). DSGVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen

Person [Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject]. In P. Gola (Ed.), *Datenschutz-Grundverordnung: DS-GVO. VO (EU) 2016/679 [General Data Protection Regulation: GDPR. REGULATION (EU) 2016/679]* (2nd ed.). C.H. Beck.

Franck, L. (2018b). DS-GVO Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person [Art. 13 GDPR Information to be provided where personal data are collected from the data subject]. In P. Gola (Ed.), *Datenschutz-Grundverordnung: DS-GVO. VO (EU) 2016/679 [General Data Protection Regulation: GDPR. REGULATION (EU) 2016/679]* (2nd ed.). C.H. Beck.

Frenzel, E. M. (2021). DS-GVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten [Art. 9 GDPR Processing of special categories of personal data]. In B. Paal & D. A. Pauly (Eds.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG [General Data Protection Regulation Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Gabriele, S., & Chiasson, S. (2020). Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In *Proceedings of the 2020 CHI Conference on human factors in computing systems* (pp. 1–12). Association for Computing Machinery. doi: 10.1145/3313831.3376651

Golland, A. (2018). Das Kopplungsverbot in der Datenschutz-Grundverordnung [Prohibition of tying in the General Data Protection Regulation]. *MMR Zeitschrift für IT-Recht und Recht der Digitalisierung*, *21*(3), 130–135.

Greve, H. (2018). DSGVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person [Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject]. In G. Sydow (Ed.), *Europäische Datenschutzgrundverordnung. Handkommentar [European General Data Protection Regulation. Comment]* (2nd ed.). Nomos Verlagsgesellschaft; MANZ Verlag; Dike Verlag.

Herbst, T. (2020a). DS-GVO Art. 4 Abs. 2 Verarbeitung [Art. 4(2) GDPR Processing]. In J. Kühling & M. Buchner (Eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG [General Data Protection Regulation, Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Herbst, T. (2020b). DS-GVO Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten [Art. 5 GDPR Principles relating to processing of personal data]. In J. Kühling & M. Buchner (Eds.), *Datenschutz-*

Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG [General Data Protection Regulation, Federal Data Protection Act] (3rd ed.). C.H. Beck.

Hill, A. D., Kern, D. A., & White, M. A. (2012). Building understanding in strategy research: The importance of employing consistent terminology and convergent measures. *Strategic Organization*, *10*(2), 187-200. doi: 10.1177/1476127012445239

Holst, A. (2021). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025.* Retrieved from `https://www.statista.com/statistics/871513/worldwide-data-created/` (Accessed on January 16, 2022)

Information Commissioner's Office. (n.d.). *Principle (b): Purpose limitation.* Retrieved from `https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/` (Accessed on February 28, 2022)

Ingold, A. (2018). DSGVO Art. 7 Bedingungen für die Einwilligung [Art. 7 GDPR Conditions for consent]. In G. Sydow (Ed.), *Europäische Datenschutzgrundverordnung: Handkommentar [European General Data Protection Regulation. Comment]* (2nd ed.). Nomos Verlagsgesellschaft; MANZ Verlag; Dike Verlag.

Jóri, A. (2019). Hungary: Introduction to the GDPR Application and a Brief History of Data Protection. *European Data Protection Law (EDPL)*, *5*(4), 528–532. doi: 10.21552/edpl/2019/4/11

Kao, Y.-S., Nawata, K., & Huang, C.-Y. (2019). An Exploration and Confirmation of the Factors Influencing Adoption of IoT-Based Wearable Fitness Trackers. *International Journal of Environmental Research and Public Health*, *16*(18), 3227. doi: 10.3390/ijerph16183227

Kästle-Lamparter, D. (2016). *Welt der Kommentare: Struktur, Funktion und Stellenwert juristischer Kommentare in Geschichte und Gegenwart [World of comments: Structure, function and significance of legal comments in the past and present]* (1st ed.). Mohr Siebeck.

Klar, M., & Kühling, J. (2020). DS-GVO Art. 4 Abs. 1 personenbezogene Daten (inkl. betroffene Person [Art. 4(1) GDPR Personal data]. In J. Kühling & M. Buchner (Eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG [General Data Protection Regulation, Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Koytcheva, M., & Gebbie, L. (2021). *Good Times for the Smart Wearables Market.* Retrieved from `https://my.ccsinsight.com/reportaction/D22615/Toc?SearchTerms=fitness%20tracker` (Accessed on April 03, 2022)

Krishnamurthy, V. (2020). A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. *AJIL Unbound*, *114*, 26–30. doi: 10.1017/aju.2019.79

Krohm, N., & Müller-Peltzer, P. (2017). Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung. Das Aus für das Modell "Service gegen Daten"? [Effects of the prohibition of tying on the practicability of consent. The end for the "service for data" model?]. *ZD Zeitschrift für Datenschutz*, 7(12), 551–556.

Kühling, J., & Buchner, B. (2020). DS-GVO Art. 7 Bedingungen für die Einwilligung [Art. 7 GDPR Conditions for consent]. In J. Kühling & B. Buchner (Eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG [General Data Protection Regulation, Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Kühling, J., & Raab, J. (2020). DS-GVO Art. 2 Sachlicher Anwendungsbereich [Art. 2 GDPR Material scope]. In J. Kühling & M. Buchner (Eds.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG [General Data Protection Regulation, Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Lachaud, E. (2020). ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification. *European Data Protection Law Review (Internet)*, *6*(2), 194–210. doi: 10.21552/edpl/2020/2/7

Lee, S. Y., & Lee, K. (2018). Factors that influence an individual's intention to adopt a wearable healthcare device: The case of a wearable fitness tracker. *Technological Forecasting and Social Change*, *129*, 154-163. doi: 10.1016/j.techfore.2018.01.002

Lin, T., Omata, M., Hu, W., & Imamiya, A. (2005). Do physiological data relate to traditional usability indexes? In *Proceedings of the 17th Australia Conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future* (pp. 1–10). Computer-Human Interaction Special Interest Group (CHISIG) of Australia.

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2018). *The Privacy Policy Landscape After the GDPR.* arXiv. doi: 10.48550/ARXIV.1809.08396

Litman-Navarro, K. (2019). *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.* Retrieved from `https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html` (Accessed on January 16, 2022)

Matejek, M., & Mäusezahl, S. (2019). Gewöhnliche vs. sensible personenbezogene Daten. Abgrenzung und Verarbeitungsrahmen von Daten gem. Art. 9 DS-GVO [Ordinary vs. sensitive personal data. Delimita-

tion and processing framework of data according to Art. 9 GDPR]. *ZD Zeitschrift für Datenschutz*, *9*(12), 551–556.

McDonald, A. M., & Cranor, L. F. (2008). The Cost of Reading Privacy Policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*, 543.

McGinnis, J. O., & Rappaport, M. B. (2017). The Constitution and the Language of the Law. *William and Mary Law Review*, *59*, 1321.

McMeekin, N., Wu, O., Germeni, E., & Briggs, A. (2020). How methodological frameworks are being developed: evidence from a scoping review. *BMC Medical Research Methodology*, *20*(1), 173. doi: 10.1186/s12874-020-01061-4

Mesarčík, M. (2020). Apply or not to apply?: A Comparative View on Territorial Application of CCPA and GDPR. *Bratislava Law Review*, *4*, 81-94. doi: 10.46282/blr.2020.4.2.171

Meyers, W. A. (2019). C is for cookie: Is the EU's new "cookie law" good enough to protect my data? *The International lawyer*, *52*(3), 491–514.

Mohan, J., Wasserman, M., & Chidambaram, V. (2019). Analyzing GDPR Compliance Through the Lens of Privacy Policy. In V. Gadepally et al. (Eds.), *Heterogeneous Data Management, Polystores, and Analytics for Healthcare* (pp. 82–95). Springer International Publishing. doi: 10.1007/978-3-030-33752-0_6

Morel, V., & Pardo, R. (2020). SoK: Three Facets of Privacy Policies. In *Proceedings of the 19th workshop on privacy in the electronic society* (pp. 41–56). Association for Computing Machinery. doi: 10.1145/3411497.3420216

Paal, B., & Hennemann, M. (2021). DS-GVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person [Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject]. In B. Paal & D. A. Pauly (Eds.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG [General Data Protection Regulation Federal Data Protection Act]* (3rd ed.). C.H. Beck.

Petri, T. (2019). DSGVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten [Art. 9 GDPR Processing of special categories of personal data]. In S. Simitis, G. Hornung, & I. Spiecker (Eds.), *Datenschutzrecht. DSGVO mit BDSG [Data protection law. GDPR with BDSG]* (1st ed.). Nomos Verlagsgesellschaft.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1). doi: 10.1093/cybsec/tyy001

Pollach, I. (2007). What's wrong with online privacy policies? *Communica-*

tions of the ACM, *50*(9), 103-108. doi: 10.1145/1284621.1284627

Quaas, S. (2021). DSGVO Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person [Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject]. In A. Wolff & S. Brink (Eds.), *Bek'sche Online-Kommentare [Beck's online comments]* (39th ed.). C.H. Beck.

Reidenberg, J., Breaux, T., Cranor, L., French, B., Grannis, A., Graves, J., ... Schaub, F. (2014). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2418297

Reimer, P. (2018). DSGVO Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten [Art. 5 GDPR Principles relating to processing of personal data]. In G. Sydow (Ed.), *Europäische Datenschutzgrundverordnung: Handkommentar [European General Data Protection Regulation. Comment]* (2nd ed.). Nomos Verlagsgesellschaft; MANZ Verlag; Dike Verlag.

Ryngaert, C., & Taylor, M. (2020). The GDPR as Global Data Protection Regulation? *AJIL Unbound*, *114*, 5-9. doi: 10.1017/aju.2019.80

Safari, B. A. (2017). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. *Seton Hall Law Review*, *47*(3), 809.

Sageder, D. (2010). Terminology Today: A Science, an Art or a Practice? Some Aspects on Terminology and Its Development. *Brno studies in English*, *36*(1), 123.

Sánchez, D., Viejo, A., & Batet, M. (2021, 02). Automatic Assessment of Privacy Policies under the GDPR. *Applied Sciences*, *11*, 1762. doi: 10.3390/app11041762

Schantz, P. (2017). Die unterschiedlichen Kodifikationen des Datenschutzrechts [The different codifications of data protection law]. In P. Schantz & H. A. Wolff (Eds.), *Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis [The new data protection law. General Data Protection Regulation and the Federal Data Protection Act in practice]* (1st ed.). C.H. Beck.

Schiff, A. (2018). DS-GVO Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten [Art. 9 GDPR Processing of special categories of personal data]. In E. Ehmann & M. Selmayr (Eds.), *Datenschutz-Grundverordnung: DS-GVO [General Data Protection Regulation: GDPR]* (2nd ed.). C.H. Beck.

Schild, H. H. (2021). DSGVO Art. 4 Begriffsbestimmungen [Art. 4

GDPR Definitions]. In A. Wolff & S. Brink (Eds.), *Bek'sche Online-Kommentare [Beck's online comments]* (39th ed.). C.H. Beck.

Schneider, J. (2017). Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus? [Does Art. 9 GDPR exclude the permissibility of processing in the case of big data?]. *ZD Zeitschrift für Datenschutz*, *7*(7), 303–308.

Schulz, S. (2018). DS-GVO Art. 7 Bedingungen für die Einwilligung [Art. 7 GDPR Conditions for consent]. In P. Gola (Ed.), *Datenschutz-Grundverordnung: DS-GVO. VO (EU) 2016/679 [General Data Protection Regulation: GDPR. REGULATION (EU) 2016/679]* (2nd ed.). C.H. Beck.

Schuster, F., & Dalby, L. (2019). DS-GVO Art. 2 Sachlicher Anwendungsbereich [Art. 2 GDPR Material scope]. In G. Spindler & F. Schuster (Eds.), *Recht der elektronischen Medien [Electronic media law]* (4th ed.). C.H. Beck.

Sheffield Hallam University. (n.d.). *Privacy Notice for Research Participants.* Retrieved from `shu.ac.uk/about-this-website/privacy-policy/privacy-notices/privacy-notice-for-research` (Accessed on April 28, 2022)

Soames, S. (2011). Toward a Theory of Legal Interpretation. *NYU Journal of Law Liberty*, *6*(2), 1. doi: 10.23943/princeton/9780691160726.003.0014

Squires, H., Chilcott, J., Akehurst, R., Burr, J., & Kelly, M. P. (2016). A Framework for Developing the Structure of Public Health Economic Models. *Value in Health*, *19*(5), 588-601. doi: 10.1016/j.jval.2016.02.011

Stake, R. E. (1999). *The Art of Case Study Research* (6th ed.). Sage Publications.

Stemmer, B. (2021). DS-GVO Art. 7 Bedingungen für die Einwilligung [Art. 7 GDPR Conditions for consent]. In A. Wolff & S. Brink (Eds.), *Bek'sche Online-Kommentare [Beck's online comments]* (37th ed.). C.H. Beck.

Sury, U. (2021). Die unterbewertete Datenschutzerklärung [The underrated privacy policy]. *Informatik-Spektrum*, *44*(6), 459–460.

Torraco, R. J. (2005). Writing Integrative Literature Reviews: Guidelines and Examples. *Human Resource Development Review*, *4*(3), 356-367. doi: 10.1177/1534484305278283

Tzanou, M. (2020). *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (1st ed.). Routledge. doi: 10.4324/9780429022241

Uecker, P. (2019). Extraterritorialer Anwendungsbereich der DS-GVO. Erläuterungen zu den neuen Regelungen und Ausblick auf internationale

Entwicklungen [Extraterritorial scope of application of the GDPR. Explanations of the new regulations and outlook on international developments]. *ZD Zeitschrift für Datenschutz*, *9*(2), 67–71.

Vailshery, L. S. (2020). *Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025.* Retrieved from `https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/` (Accessed on January 16, 2022)

van Mil, J. W. F., & Henman, M. (2016). Terminology, the importance of defining. *International Journal of Clinical Pharmacy*, *38*(3), 709–713. doi: 10.1007/s11096-016-0294-5

Vienna University of Economics and Business. (2019). *WUPOL Website Privacy Policy.* Retrieved from `https://www.wu.ac.at/fileadmin/wu/h/datenschutz/WUPOL_Website-Datenschutzrichtlinie.pdf` (Accessed on April 28, 2022)

Voigt, P., & von dem Busche, A. (2018). *EU-Datenschutz-Grundverordnung (DSGVO). Praktikerhandbuch [General Data Protection Regulation (GDPR). Practitioner's handbook]* (1st ed.). Springer Verlag.

Waldman, A. E. (2018). Privacy, Notice and Design. *Stanford Technology Law Review*, *21*(1), 74–127. doi: 10.2139/ssrn.2780305

WP 29. (2011). *Opinion 15/2011 on the definition of consent.* Retrieved from `https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf` (Accessed on December 20, 2021)

WP 29. (2013). *Opinion 03/2013 on purpose limitation.* Retrieved from `https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf` (Accessed on December 20, 2021)

WP 29. (2018). *Guidelines on transparency under regulation 2016/679.* Retrieved from `https://ec.europa.eu/newsroom/article29/items/622227/en` (Accessed on April 30, 2022)

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *SIGMIS Database*, *40*(1), 38-51. doi: 10.1145/1496930.1496937

Yin, R. K. (2014). *Case Study Research: Design and Methods* (5th ed.). SAGE Publications.

Zaeem, R. N., & Barber, K. S. (2020). The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. *ACM Transactions on Management Information Systems*, *12*(1). doi: 10.1145/3389685

Zimmeck, S., & Bellovin, S. M. (2014, August). Privee: An Architecture for Automatically Analyzing Web Privacy Policies. In *23rd USENIX*

Security Symposium (USENIX Security 14) (pp. 1–16). USENIX Association. Retrieved from `https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/zimmeck`

Zimmermann, R. (2020). Privatrechtliche Kommentare im internationalen Vergleich. Verbreitung, Varianz, Verwandtschaft [Private law comments in international comparison. Distribution, variance, relationship]. In D. Kästle-Lamparter, N. Jansen, & R. Zimmermann (Eds.), *Juristische Kommentare: Ein internationaler Vergleich [Legal comments: An international comparison].* Mohr Siebeck.

Appendix A Privacy Policy Appraisal Framework (PPAF)

Guideline on the PPAF's aspects and corresponding parameters for the identification of terms related to the GDPR's material scope and legal grounds for personal data processing

Aspect 1 – Display of privacy policies
How easily accessible are privacy policies? How is the information displayed in privacy policies?
Aspect 2 – Information of privacy policies
Is there a specific reference to personal data? Are the types of personal data mentioned according to Art. 4(1) GDPR and Art. 9(1) GDPR? Is the processing of personal data referred to as processing of personal data? Is the processing of special categories of personal data explicitly and separately mentioned? Are the reasons for personal data processing defined as purposes? Are the legal grounds for the processing of personal data mentioned in the privacy policy according to Art. 6(1) GDPR and Art. 9(2) GDPR?
Aspect 3 – Understandability of privacy policies
Are legal terms explained using clear and plain language?