universität
uulm

Faculty of Engineering Sciences, Computer Science and Psychology
Institute of Databases and Information Systems

Impact of the GDPR on the Development of eHealth Software

Bachelor Thesis at Ulm University

Submitted By:
Mahatir Muhammad Said
mahatir.said@uni-ulm.de
946684

Reviewer:
Prof. Dr. Manfred Reichert

Supervisor:
Robin Kraft

2022

Version June 24, 2022

Satz: PDF-LaTeX 2$_\varepsilon$

Abstract

The new EU General Data Protection Regulation (GDPR) became effective on May 25, 2018 and regulates how personal data may be processed by companies, government agencies and other organizations in the European Union (EU). Since prior research focused mostly on the GDPR in general, its implications and impact on the development of health software are not as intuitive as one may think. Even though our main goal was to analyze the impact of the GDPR on health software, we have simultaneously covered several other important aspects of complying with the GDPR by researching relevant literature. We have outlined the history and content of the GDPR as well as other regulations like the Federal Data Protection Act (FDPA) and put them into the context of health. As a result, we were able to identify best practices for health-app providers and possibilities on how to comply with specific key aspects of the GDPR. Several other regulations and norms have been considered and illustrated concisely in this thesis. We have subsequently applied or analysis on eSano, the health platform of the University of Ulm. Our results show that eSano is GDPR-compliant with minor room for improvement.

Acknowledgements

I want to thank everyone who supported me throughout this thesis. First and foremost, my thanks go to the reviewer of this thesis, Prof. Dr. Manfred Reichert who is a lecturer at the University of Ulm. I would also like to thank my family for proofreading this work.

I want to thank the eSano team for their continuous support. A special thanks goes to Robin Kraft, who supervised this thesis and always provided me with insightful guidance and support.

Contents

1 Introduction **3**
- 1.1 Motivation . . . 3
- 1.2 Problem Statement . . . 4
- 1.3 Objective of the thesis . . . 5
- 1.4 Structure of the thesis . . . 6

2 Fundamentals **7**
- 2.1 General Data Protection Regulation . . . 7
  - 2.1.1 History and territorial scope . . . 7
  - 2.1.2 GDPR vs US legislation . . . 11
  - 2.1.3 Key principles . . . 13
- 2.2 eHealth platforms . . . 15
  - 2.2.1 GDPR in the health sector . . . 17
  - 2.2.2 Health-related legal bases in Germany . . . 19
  - 2.2.3 eSano as an eHealth platform of the University of Ulm . . . 21
- 2.3 Summary . . . 23

3 The GDPR and its implementation in practice **24**
- 3.1 Concise and succinct summary of the GDPR . . . 24
  - 3.1.1 Stakeholders . . . 24
  - 3.1.2 Consumer rights and possibilities . . . 26
  - 3.1.3 Data Protection Management . . . 28
  - 3.1.4 Data Protection Impact Assessment . . . 31
  - 3.1.5 Lawfulness of data processing . . . 34
- 3.2 Interfaces with other regulations . . . 35
  - 3.2.1 Differences between Data Protection Directive 95/46/EC and the GDPR . . . 35
  - 3.2.2 Federal Data Protection Act . . . 37
  - 3.2.3 Medical Device Regulation . . . 39
  - 3.2.4 Similarities and differences between GDPR and MDR . . . 42
  - 3.2.5 Other relevant standards and their relationship with the GDPR . . . 44
- 3.3 GDPR-related best practices . . . 46
  - 3.3.1 Measures to prove compliance regarding data processing 46
  - 3.3.2 Privacy Policy . . . 49
  - 3.3.3 Cookies and storage periods . . . 50
  - 3.3.4 Requirements for a deletion concept . . . 51
  - 3.3.5 Breaches and responsible authorities . . . 52

3.4 Summary 53

4 Application of elaborated findings on eHealth platforms 54
4.1 Impact of the GDPR on the eHealth sector 54
4.1.1 Decision tree to comply with legislation 54
4.1.2 Lawful processing of patient data 56
4.1.3 Health-app providers' responsibilities in Germany 57
4.1.4 Checklist for eHealth-platform operators 58
4.2 GDPR with regard to the eHealth platform eSano 62
4.2.1 Applying the decision tree on eSano 62
4.2.2 Privacy Policy AS/IS versus TO/BE 67
4.2.3 DPIA AS/IS versus TO/BE 70
4.2.4 Applying the checklist on eSano 76
4.3 Summary 79

5 Discussion 80
5.1 Challenges 80
5.1.1 Challenges of ensuring privacy-compliant health apps . . 80
5.1.2 Issues of transferring data to other countries 81
5.2 Criticism 82
5.2.1 Complexity, time investment, and obscurity 82
5.2.2 Fines and data breaches 83
5.3 Summary 85

6 Conclusion 87
6.1 Roundup 87
6.2 Outlook 88

Bibliography 89

A Acronyms 97

B Declaration of consent 98

C eSano Privacy Policy 108

D eSano On- and Offboarding 112

E Secure Coding 113

F Risk Assessment 114

1 Introduction

Chapter 1 will introduce the importance of data in the health sector and outlines the problems we aim to solve with this thesis. The objective and structure of this thesis will give an insight into what the reader can expect.

1.1 Motivation

In the information age, the amount of data has become almost immeasurable. However, instead of rendering the sheer mass of data redundant, it makes it all the more important: since COVID-19[1], we have realized that the fight against such diseases requires the cooperation of numerous organizations which have established themselves in the field of health. Professor Alexander Radbruch and Professor Louisa Specht-Riemenschneider of the University of Bonn have published an article in the German Medical Journal “Deutsches Ärzteblatt”, which demonstrates that the analysis of large data sets holds considerable potential for research in the health sector [1]. The examination of these data sets could facilitate and improve the process of detecting and assessing illnesses. Medical experts wish for databases with large volumes of medical data, but data protection laws present high impediments to analyzing such data. The Medical Informatics Initiative of the Federal Ministry of Education and Research has worked with different entities on a template for “broad consent”, which allows patients to consent to the processing of their data for research purposes. However, this model text will only facilitate the analysis of data compiled in the future, and it only applies to Germany and not the EU. Sharing data for scientific purposes poses a difficult challenge for all actors involved because of a lack of legal certainty and the associated technical effort. To simplify the vast number of challenges related to data collection, standards for data processing must be harmonized. Here, the General Data Protection Regulation comes into action.

[1] Coronavirus Disease 2019.

The GDPR forms the basis for compliance among several countries in the EU. After more than 20 years, it replaced the outdated Data Protection Directive (DPD) [2]. Technology is growing fast, and with increasingly more data, properly handling such data becomes an inevitable task. Therefore, different EU-related parties agreed on protecting personal data in the EU. Since we are discussing personal data, particularly in the eHealth sector, a legal basis is required. eHealth is a collective term used for applications that help patients with treatment [3]. Various laws related to eHealth have been developed, such as the Patient Data Protection or the Digital Supply and Care Modernization Act. Distinctions like these aim to accelerate the progress of digitization in each area. Therefore, we explicitly differentiate between the context of health software concerning the GDPR. It is also planned to set up a national eHealth contact point in Germany in 2023 to share health data with other doctors in the EU in a secure form [3].

To apply the GDPR within the scope of this thesis, the eHealth platform of the University of Ulm, eSano, offers a good opportunity to apply the knowledge we will gain from the literature research. eSano is composed of different health-related functions and intends to enhance and improve them [4]. To continue developing eSano, one essential aspect is to analyze how the GDPR impacts the development of health-related software. What exactly the problem is and how we will face this challenge is outlined in Section 1.2.

1.2 Problem Statement

To ensure that (sensitive) data, especially in the health sector, complies with the GDPR, platform operators require a basis on which they can work. This basis is the GDPR. The impact of the GDPR on the development of health software may not be as trivial as it seems at first glance. One of the biggest challenges here is that we have to consider the interactions and interfaces with other laws and standards, such as the Medical Device Regulation (MDR). Over the past few years, the Federal Ministry of Health (FMH) has introduced a framework consisting of different platforms [5]. It aims to create a space for a structured exchange of ideas by 2025. However, with the creation of more and more frameworks and rules, developers and patients start to lose track of what is important.

Here, it is challenging to assess carefully and to implement the most critical aspects of the legislation. Even though patients profit from new technologies, it also tends to result in sharing more data with stakeholders [6]. Since almost every site contains at least some kind of informed consent, it entails a lack of care.

For instance, Amazee, a website focusing on digital performance, found that approximately four in five users ignore cookie banners[2] [7]. The exact number of users also close those settings, whereas only about one-tenth accept them. The wide range of information and possibilities should not be underestimated. For companies, web- and app developers, usually, the expertise of a consultant must be called upon. This is for the following reasons, among others:

- plenty of room for interpretation: as mentioned above, the GDPR needs to be flexible enough to handle crises because one cannot just change their application from one day to another.
- special definitions, especially in the legal scope, are difficult to understand.
- unclarity regarding which data can be collected and when the GDPR applies due to misinformation on the internet.
- overlap with other regulations, such as the MDR or the FDPA, and it is unclear where to draw the line.
- constant new changes in legislation due to technological progress are not being appropriately addressed.
- high costs in the event of a breach.

1.3 Objective of the thesis

This thesis aims to provide a concise summary and application of the GDPR on health software. By examining the status quo, we aim to assess interdependencies between legislations like the GDPR and the FDPA.

It is challenging to cover all compliance aspects when it comes to developing health software. We will identify and focus on the most important articles and conditions for processing user data to facilitate this task. The objective is to propose recommendations to companies and institutions that develop eHealth software. These suggestions should be extracted from different sources and build the basis for a framework that allows stakeholders to check their apps for conformity.

[2]The dataset considered website views (n = 100,000).

1.4 Structure of the thesis

This work aims to research the GDPR and its implementation in practice. This shall be achieved by ensuring that essential contents of the GDPR are presented compactly. To better understand how data protection regulations evolved, we will first have a look at the history of the GDPR and its relevance in the health sector in Chapter 2. The idea is that we examine the GDPR step-by-step to outline articles and recitals relevant to users and providers of (eHealth) apps in Chapter 3. Based on our reviewed literature and findings, we will establish best practices that help those responsible to implement key aspects of the GDPR. Subsequently, interfaces between other regulations such as the FDPA or the MDR will be given a summary of. We will then make a compact analysis of how the GDPR affects eHealth platforms and apply the methods outlined earlier to eSano in Chapter 4, followed by a discussion of the implications of the GDPR in Chapter 5. Last but not least, we will conclude our findings in Chapter 6. By no means will we be able to cover every single regulation in the scope of this thesis. However, we should be able to provide a decent guideline for complying with the GDPR when developing health software. The realization of this goal is to be achieved incrementally in four steps:

1. Research and analysis of the GDPR, its articles, and necessary recitals
2. Comparing how the GDPR overlaps with other regulations like the FDPA
3. Best practices for businesses to comply with rules
4. Analyzing the impact and applying the findings on eSano

The approach to this solution requires a careful evaluation of existing literature and assistance from the eSano development team. We will also try to get input from the responsible entities for the development process, i.e., the Institute of Databases and Information Systems and the health division, i.e., the Department of Clinical Psychology and Psychotherapy of the University of Ulm. Finally, we will conclude our findings with a summary and discussion regarding challenges and breaches.

2 Fundamentals

This chapter will cover several aspects of the GDPR, such as its history, the existing state of affairs regarding US legislation, and fundamental principles. We will also look at the health sector in the face of the GDPR.

2.1 General Data Protection Regulation

The GDPR replaced the Data Protection Directive 95/46/EC, enacted in 1995 [8]. Initially, it took four years – starting from 2012 – until a political agreement was reached. Once the majority of the European Parliament approved the GDPR, there was a transition period from April 2016 until May 2018, in which companies had to adapt accordingly. The enactment aimed to improve transparency while also providing an advanced framework that is capable of ensuring that data is processed under the law.

A “data subject” is a website or app visitor whose (personal) data is stored [9]. Personal data is all information that, in some way, can be traced back to a person. This includes external features and character traits as well as digital data and metadata generated through the use of online services that we call “identifiers“.

2.1.1 History and territorial scope

To get a better overview of the history of the GDPR, we have created a timeline that summarizes the most important directives and regulations (see Figure 2.1).

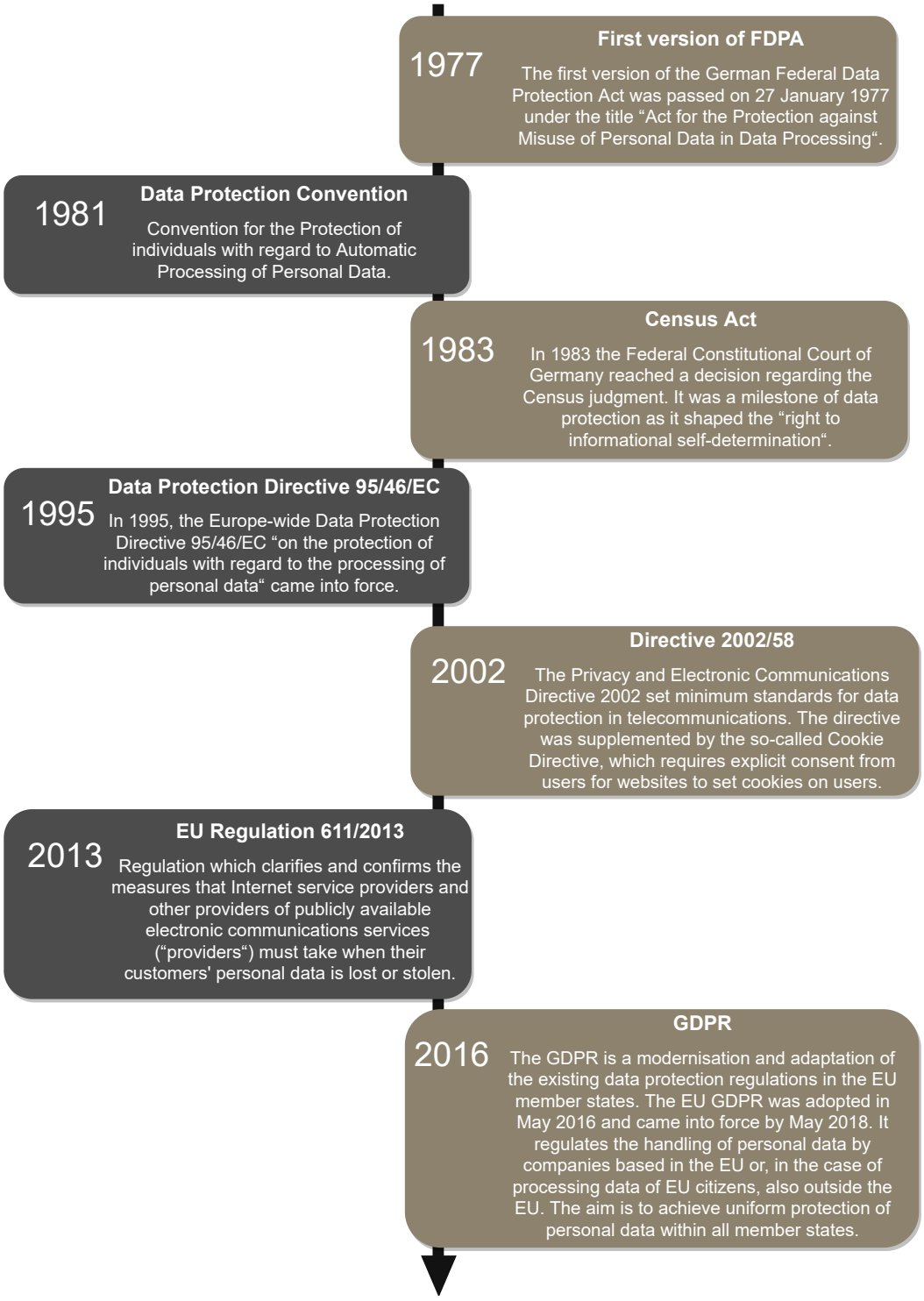


Figure 2.1: History of Directives and Regulations based on [2] and [10]

As early as 1977, Germany expressed by law that data protection is not only required but also exists as a legal right [11]. Hence, a first version of the FDPA was released in 1977. The Data Protection Directive, officially called Directive 95/46/EC, came into force in August 1995 [11]. It is about the protection of people during the processing of personal data [12]. Due to an inconsiderable number of changes in technology and the DPD being outdated, the European Commission proposed new legislations in 2012, which enhance data protection and handle the diversity of technology [13].

On March 12, 2014, the European Parliament adopted the GDPR. Out of 653 votes, 621 voted in favor of it in the plenary vote [8]. In 2015, the European Parliament, the Council, and the Commission reached an agreement. On April 27, 2016, the Regulation (EU) 2016/679 and the Directive 95/46/EC, representing the GDPR, were published and since May 25, 2018, the General Data Protection Regulation applies.

The EU consists of 27 European countries or member states. Figure 2.2 shows those countries and membership aspirants like Turkey. It also depicts DPA's across Europe and where the GDPR applies. We differentiate between national and lower-level data protection authorities (DPA). The GDPR refers to the former as "lead supervisory authority" in Art. 56(1) [9], which is the Single Point of Contact (SPoC) for data controllers in case they want to process data from a third-party country. The lead supervisory authority cooperates with other supervisory authorities under Art. 60(1) GDPR. Germany consists of 16 federal states and each state has a different responsible authority which can be seen by the blue dots in Figure 2.2. Since December 31, 2020, the GDPR does not apply to England anymore [14]. Organizations in the UK have to comply with the Data Protection Act 2018. The key principles remained the same, and companies in the European Economic Area (EEA) can still receive personal data.

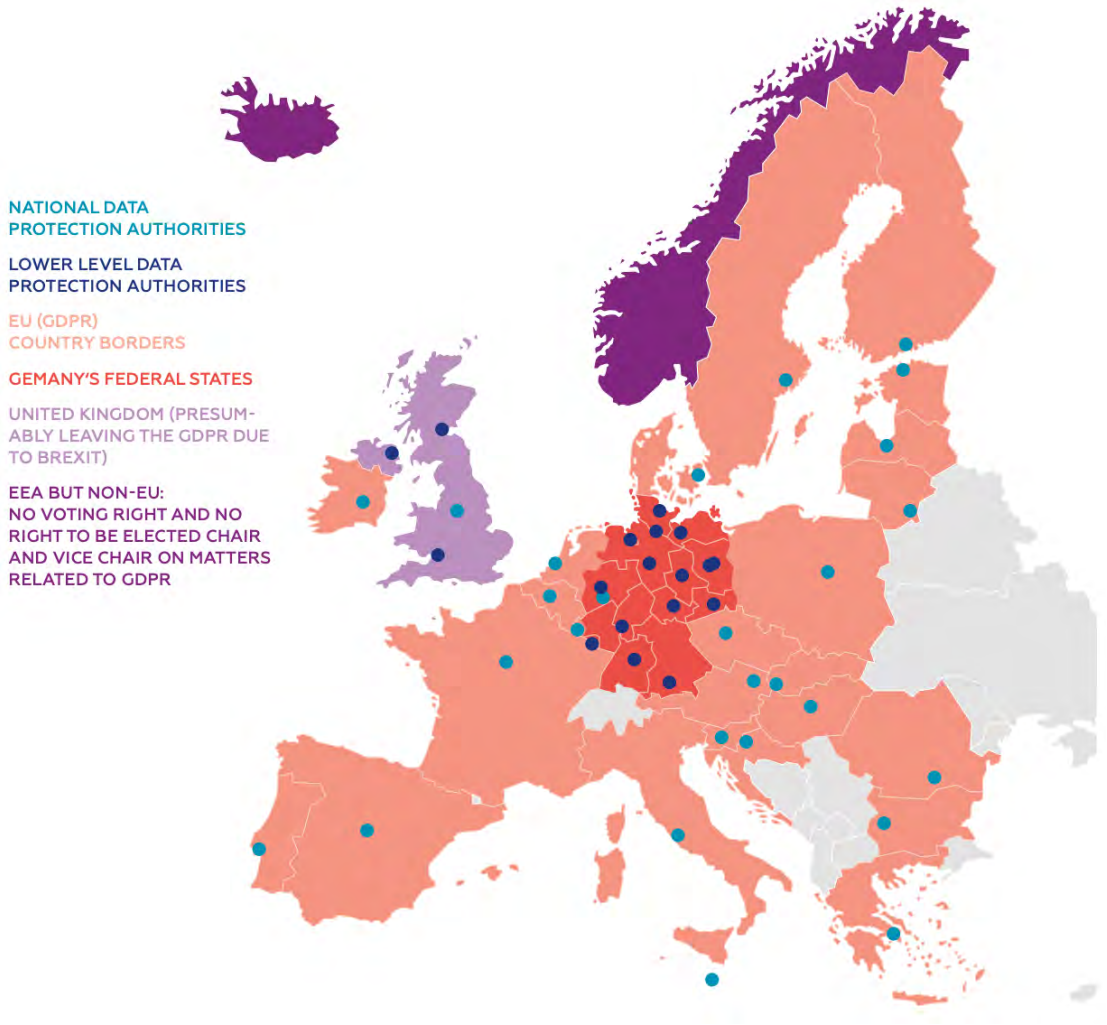


Figure 2.2: Europe and the scope of the GDPR from [15]

The GDPR also does not apply in Swiss [16]. The FDPA is the data protection law of Switzerland that dates back to 1992. Since it is outdated, it is planned to introduce a revised FDPA by September 2023 which is also GDPR-compatible.

The third article of the GDPR already answers the question as to where it applies [9]. The GDPR also applies to organizations that process citizens' data in the EU, even if they are not in the EU. A non-EU company should aim to be GDPR-compliant if it addresses customers in the EU. This could be the case if, for example, a Turkish company has created German advertising on a website. If that company monitors behavior by tracking data like IP, it also falls under the scope of the GDPR. However, European regulators can not check who visits

which web page due to the sheer number of websites. Nonetheless, companies should be held accountable for tracking said data.

2.1.2 GDPR vs US legislation

In contrast to the EU, the US does not have a federal law responsible for how data is managed [12]. However, some states have laws regulating data just like the GDPR, such as Virginia and California. Since the US and the EU have a very close relationship, the US arranged the so-called “Safe Harbor Framework” in 2000, allowing companies to transmit personal data from the EU. At the beginning of the 21st century, the internet was still uncharted territory, so the “EU-US Privacy Shield” was agreed upon [17]. It came into force in 2016. For now, we will not discuss the details of that framework since the court of justice of the EU declared it invalid in July 2020, but we will refer to it later in Section 5.1.2.

To depict the difference between federal, state, and branch-specific laws, we can look at the distinction seen in Figure 2.3.

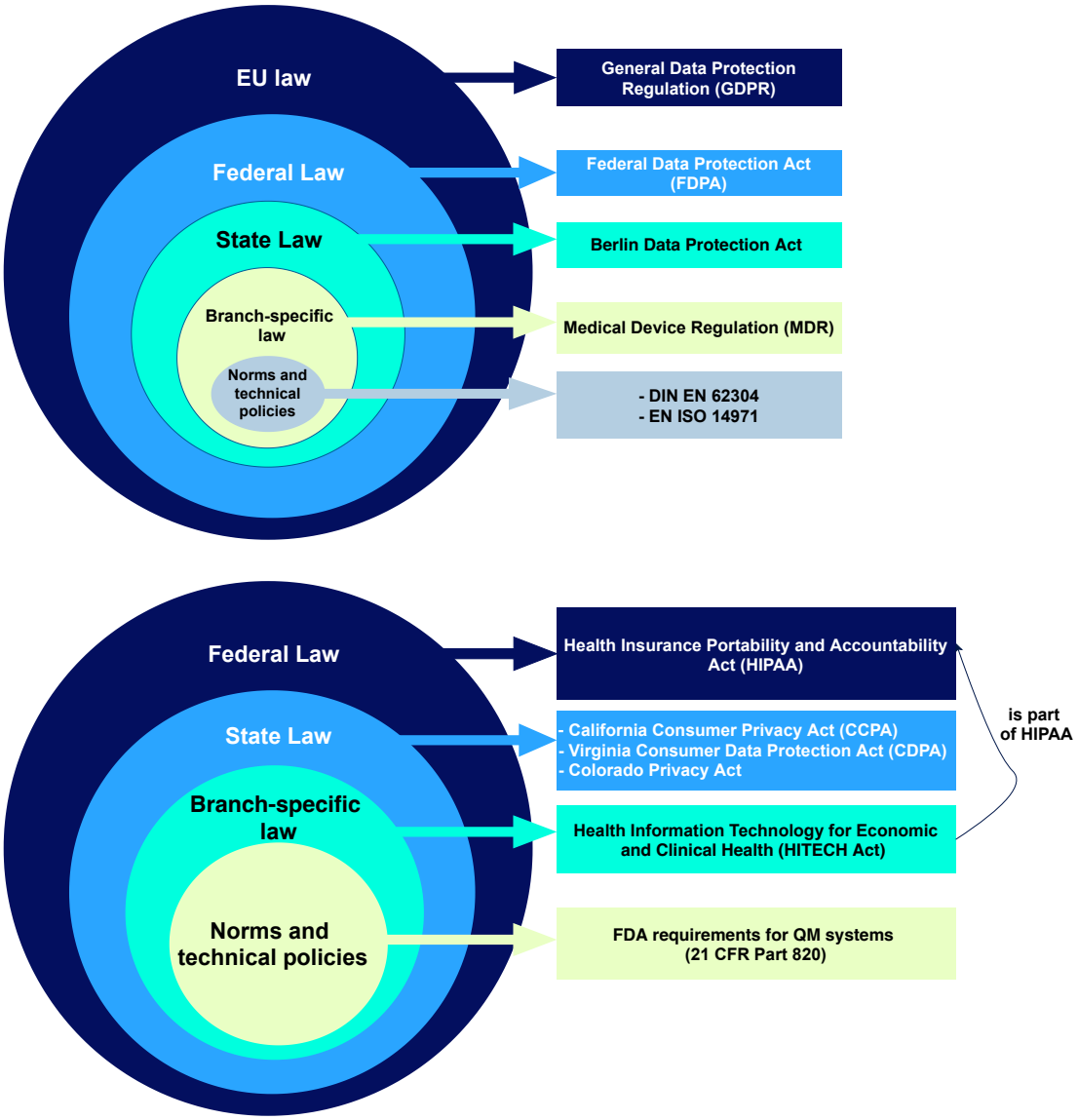


Figure 2.3: EU vs. US based on [18], [19] and [20]

HIPAA stands for the Healthcare Insurance Portability and Accountability Act, a US law passed in 1996 that addresses the protection of personally identifiable health information [21]. Under HIPAA compliance requirements, healthcare providers (e.g., hospitals, nursing facilities) and their business associates must implement rules and regulations regarding handling confidential patient data to ensure its protection. This includes any data that relates to a patient's health status and medical care and treatment costs, which means that it is any information that can be used to identify an individual.

Examples of personal health information are:

- names and addresses
- birth and death dates
- telephone and fax numbers, e-mail addresses
- social security numbers

While HIPAA represents a federal law, the California Consumer Privacy Act (CCPA) applies to California only since 2020 [22]. It governs how companies worldwide should handle the personal information of Californian residents. The key difference between the CCPA and the GDPR is that the former uses an opt-out model while the latter applies an opt-in model. In an opt-out model, the user does not have to consent to the data processing, but is entitled to object to this by "opting out". On the contrary, organizations require explicit consent from users before collecting and processing personal data – therefore, the term "opt-in".

In 2023, the new California Privacy Rights Act (CPRA) will be enacted [23]. It imposes additional responsibilities on companies related to personal data. For instance, while the CCPA included the right to delete and opt out, the CPRA gives users even more rights, such as the right to correction and nondiscrimination. With ever-changing rules, the approval of the CPRA proves that end users are welcoming more rights and even advocating to get them enforced as soon as possible.

2.1.3 Key principles

The fifth article of the GDPR defines seven principles that prescribe how personal data should be handled [9]. They are not just tentative principles, and in fact, their violation can be punished with the maximum fine under the GDPR following Art. 83(5)(a) of the GDPR. Companies should therefore familiarize their employees with the following principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy

5. Storage limitation
6. Integrity and confidentiality
7. Accountability

In the following, we will elaborate on each principle.

The first principle (“Lawfulness, fairness and transparency”) orders one to handle personal data lawfully [9]. It intends to ensure that users can exercise their rights and their right to informational self-determination. According to the GDPR, one should act to the best of one’s knowledge and belief. Data processing should be understandable for customers, which implies that one should be as transparent as possible when informing them about what happens with their data. Art. 12 of the GDPR further specifies transparency by referring to information obligations when collecting personal data. Following Art. 13(4) of the GDPR, there is no information obligation if the user already has the information. Data protection by design and by default are also intended to ensure transparency (see Art. 25 GDPR, Recital 78). In addition, there are certification procedures and data protection seals that provide data subjects with a quick overview of the level of data protection of relevant products and services. These are explained in more detail in Art. 42 and Recital 100 of the GDPR.

The Purpose limitation principle describes what exactly collected data should be used for [9]. The purpose must be clear to legitimize the processing of personal data, and it is prohibited to use the data for any other purpose. The objectives of data processing must already be defined, unambiguous and legitimate at the time of collection of personal data. Further processing for other purposes is possible if it is not incompatible with the original collection purpose and if a legal basis for this exists. The principle of data minimization means that the responsible person should limit the collection of personal data to information that is of direct relevance and necessary to fulfill a specific purpose. In addition, one should collect only the personal data needed and retain it for only as long as needed [9].

According to the fourth principle (“Accuracy”), personal data must be factually correct and up-to-date [9]. Therefore, the responsible person has to collect accurate data, and they must ensure that the data is updated promptly when a change occurs. Personal data which are inaccurate with regard to the purposes of their processing should be deleted (see, for example, Art. 17(1)(d) GDPR) or rectified immediately (Art. 16 GDPR).

The storage limitation principle states that personal data may only be stored in a form that permits identification of the individual for as long as is necessary for the processing [9]. As soon as the storage of personal data is no longer

required for processing, the personal data must be deleted (Art. 17(1)(a) GDPR), or the identification of the data subject must be removed. Exceptions arise, for example, for archiving purposes in the public interest, for scientific, historical, or statistical research purposes.

Data processing principles include integrity and confidentiality, which state that personal data must be processed so that its integrity and confidentiality are adequately guaranteed [9]. This also includes that unauthorized persons cannot access the data and cannot use either the data or their devices for processing. In this context, unauthorized persons refers to outsiders and people within the company. This is because not every employee in the company needs access to personnel data, customer data or data of other persons. To be able to guarantee the principle of integrity and confidentiality, action is required by the responsible party itself by also introducing suitable Technical and Organizational Measures (TOM) within its company. We will elaborate on these measures in Section 3.1.3.

Last but not least, the principle of accountability requires companies to follow the directions stated above [9]. Upon request, they should be able to demonstrate what they have done as well as the effectiveness of their actions. This can also be done via TOM.

Besides, purpose limitation and storage limitation refer to Art. 89(1), which defines the purposes' wherefore personal data can be processed [24]. This is because the EU had to define user rights' for more extensive collections of personal data. For instance, when it comes to health software, clinical trials require collecting large amounts of personal data. Data is usually stored in databases, and physicians often enter medication orders electronically. The collection of considerable chunks of data can thus be used to get better diagnoses and to improve the quality of treatment. Since the data is being used for scientific research, it provides a reasonable exception under Art. 89.

2.2 eHealth platforms

The term "eHealth" (electronic health) covers all healthcare applications using modern information and communication technologies, while "mHealth" (mobile health) is a subfield of eHealth [25]. The latter comprises private and public health care medical support using mobile devices and applications. The term "Big Data" refers to the processing of large (unstructured) amounts of data to gain new insights and connections [26].

The study “Further development of the eHealth strategy” [1], which PwC Strategy prepared on behalf of the German Federal Ministry of Health, discusses two topics [27]: it examines the overall conditions to further develop eHealth and based on that, it deals with the question of how the ever-increasing digitization can be used to implement new structures and processes in the healthcare system. The opportunities, challenges, and risks of individual technological developments are systematically and comprehensively analyzed with the involvement of key players in the healthcare sector.

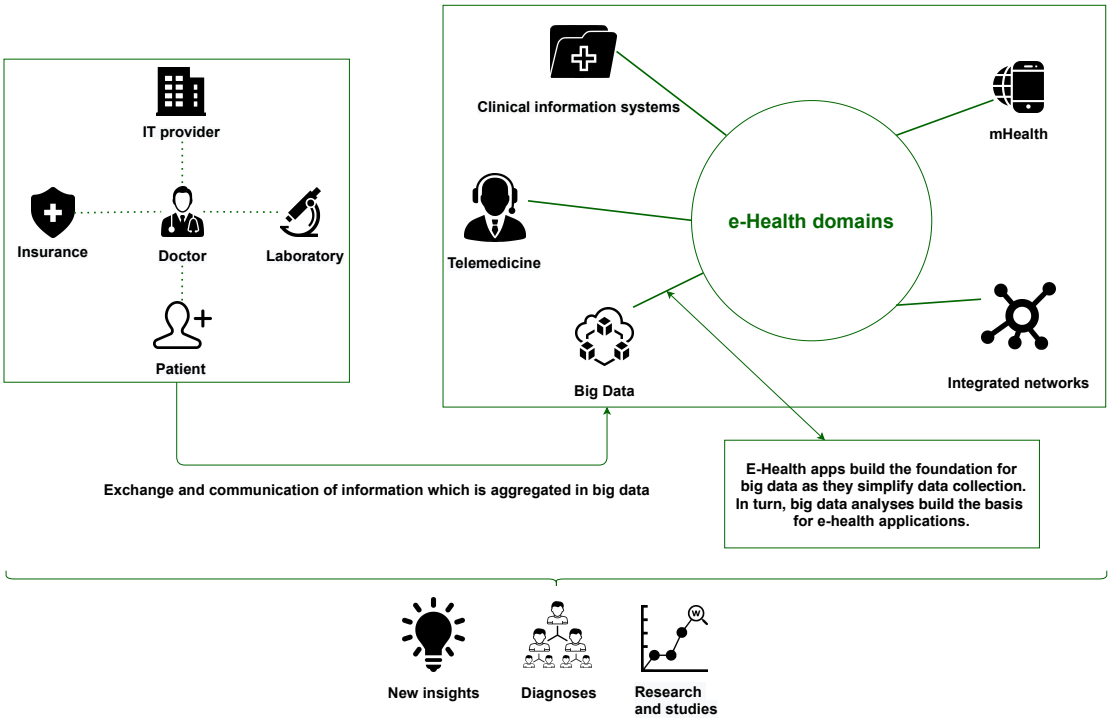


Figure 2.4: Interdependencies between eHealth and its domains based on [27], [28] and [25]

We have illustrated the application areas and interactions of eHealth and Big Data in Figure 2.4. It shows that eHealth is built on different entities that exchange information. Based on this exchange of data, databases can be created, which could then lead to gaining knowledge in several areas, such as health.

Big Data is used for research purposes in the healthcare industry, such as improving care or planning resources more efficiently in a hospital [27]. The primary source of Big Data collection is tracking, where devices such as smartphones continuously collect specific data and transmit it, sometimes in real-time,

[1] Translated accordingly.

to servers or providers. Personal data can be collected via various tracking methods, which are constantly evolving and differ depending on desktop or mobile usage. When visiting websites, the most common tool is browser cookies, which are stored on a user's terminal device (e.g., computer, tablet, smartphone) and allow users to be recognized. In addition to cookies, there are other methods, e.g., fingerprinting[2], eTag[3], and local storage[4] [29].

2.2.1 GDPR in the health sector

The availability and security of data are particularly relevant in the healthcare sector: knowledge of previous illnesses, previous treatments, and medications can be vital in individual cases and must not be lost under any circumstances, for example, through a data leakage of an insecure patient file. A system failure, e.g., the (temporary) unavailability of data could pose a significant health risk by causing treatments to be incorrect, delayed, or mistakenly to be not carried out at all.

The GDPR distinguishes between three specific types of personal data in Section 4 No. 13-15 [9]:

- genetic data
- biometric data
- health data

Genetic data are personal data relating to genetic characteristics that provide information about that person's condition [9]. Biometrics, on the other hand, are biological measurements or physical features which may be used to identify people. Health data refers to a person's physical or mental health. The 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". [9, Art. 4]

Recitals of the GDPR are not part of the legal text [30]. Instead, they precede the articles of the GDPR. They do not have any direct effect, as they are not legally

[2] Method of data collection which converts browser settings into a hash value and creates a digital signature.

[3] Entity Tags are cache validators introduced with HTTP 1.1 which help the browser to determine whether a requested resource can be retrieved from the local cache or whether the resource must be retrieved from the server again.

[4] The local storage is a property that allows websites to save information as key/value pairs, i.e., as a string.

binding. Nevertheless, the recitals are of central importance in data protection as they can be used to interpret indefinite articles. The GDPR also addresses the notion of health data in Recital 35 [9].

According to Art. 6(1) GDPR, the lawfulness of data processing can be achieved by consent which must be freely given, specific and unambiguous. The special handling of scientific data is referred to several times, for instance, in Art. 9(2)(h) and Art. 17(3)(d). In particular, Art. 9(2)(h) states that personal data can be processed for health care reasons if the member state laws allow them to do so. Art. 89 affirms that national regulations are permitted to process health data. The legal basis for processing eHealth data is, for example, a treatment contract, a legal authorization for data processing, or the patient's consent [31]. As per Art. 8, children under 16 are not allowed to consent without their parent's approval [9].

Even though all EU member states have national laws related to processing health data, only Germany and Denmark have recently changed those laws [32]. While 16 member states introduced further restrictions regarding the types of personal data mentioned above, eleven states have not put any other laws into place concerning this matter.

Recital 157 of the GDPR particularly states that putting together information from different sources could help to gain new insights related to diseases such as cancer and depression [9]. Given the COVID-19 pandemic, a lot of international collaboration – where patient data was shared for research purposes – has taken place [26]. Personal data must be protected, but at the same time, health data that could solve global problems and save millions of lives should not be disregarded.

For instance, stakeholders were afraid of not complying with the law due to uncertainties on how the GDPR had to be interpreted, which significantly affected the shared amount of data [26]. Different academies, including the European Academies Science Advisory Council (EASAC)[5], elaborated on how the hurdles of sharing sensitive health data outside the EEA could be solved. This can be done by introducing new guidelines for data transfer, safeguards, and standard contractual clauses (SCC) which are contractual texts that safeguard data processing in a country outside the EEA [33]. Via Art. 45 of the GDPR (adequacy), the EU Commission can determine that a country outside the EEA has a degree of data protection provided by its legislation, which offers European citizen protection comparable to that of the GDPR [9]. If such a decision exists, data transfer to this third country is generally permitted. Art. 46 states that

[5] Represents more than 50 academies worldwide.

the data subject has guaranteed enforceable rights and effective remedies, i.e., safeguards, to protect their data with a data processor in the third country.

International companies that transfer health data in large numbers to third countries can introduce Binding Corporate Rules (BCR) per Art. 47(2) GDPR [9]. This means that a company can impose binding rules on itself, which must then be approved by the supervisory authorities. Once they are approved, they provide legitimate permission for the data transfer.

2.2.2 Health-related legal bases in Germany

According to Art. 9(2) of the GDPR, a company can process health data for statistical purposes if a separate law permits this [34]. Such a law can be found in Section 27(1) of the FDPA. If the requirements of that section are fulfilled, the prohibition of processing is lifted. In Germany, there are several state and federal laws which are named in Figure 2.5.

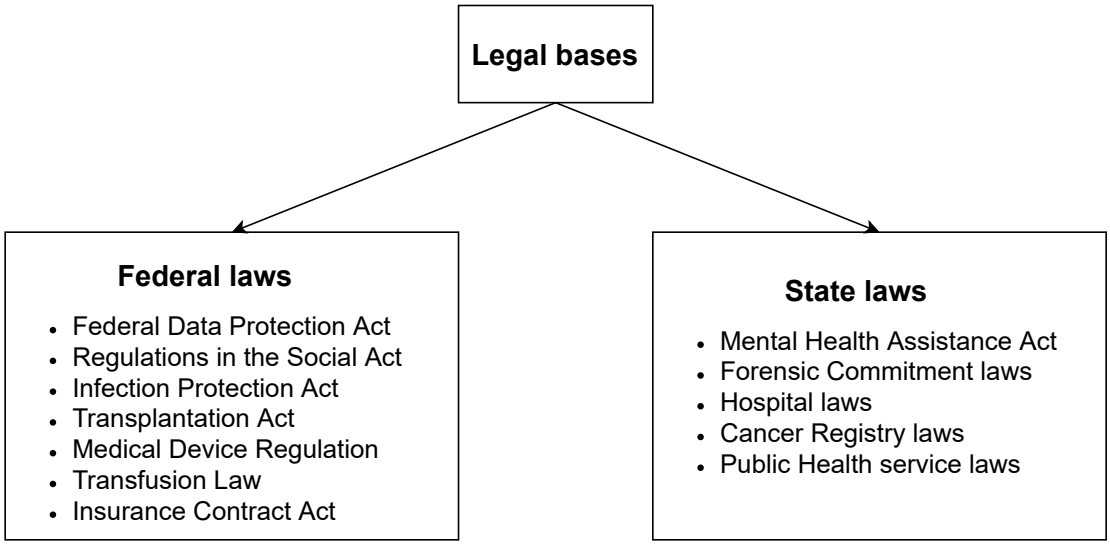


Figure 2.5: Federal and state laws in Germany in the context of health based on [34]

On the one hand, these legal bases apply depending on the type of platform that collects health data, and on the other hand, they vary by (federal) state. The relevance of these laws has become even more apparent during the COVID-19 pandemic. For instance, the application of the MDR was postponed by one year [20]. There are also numerous standards that can be used to

develop health software adequately. Their relationship is shown in the following Figure 2.6.

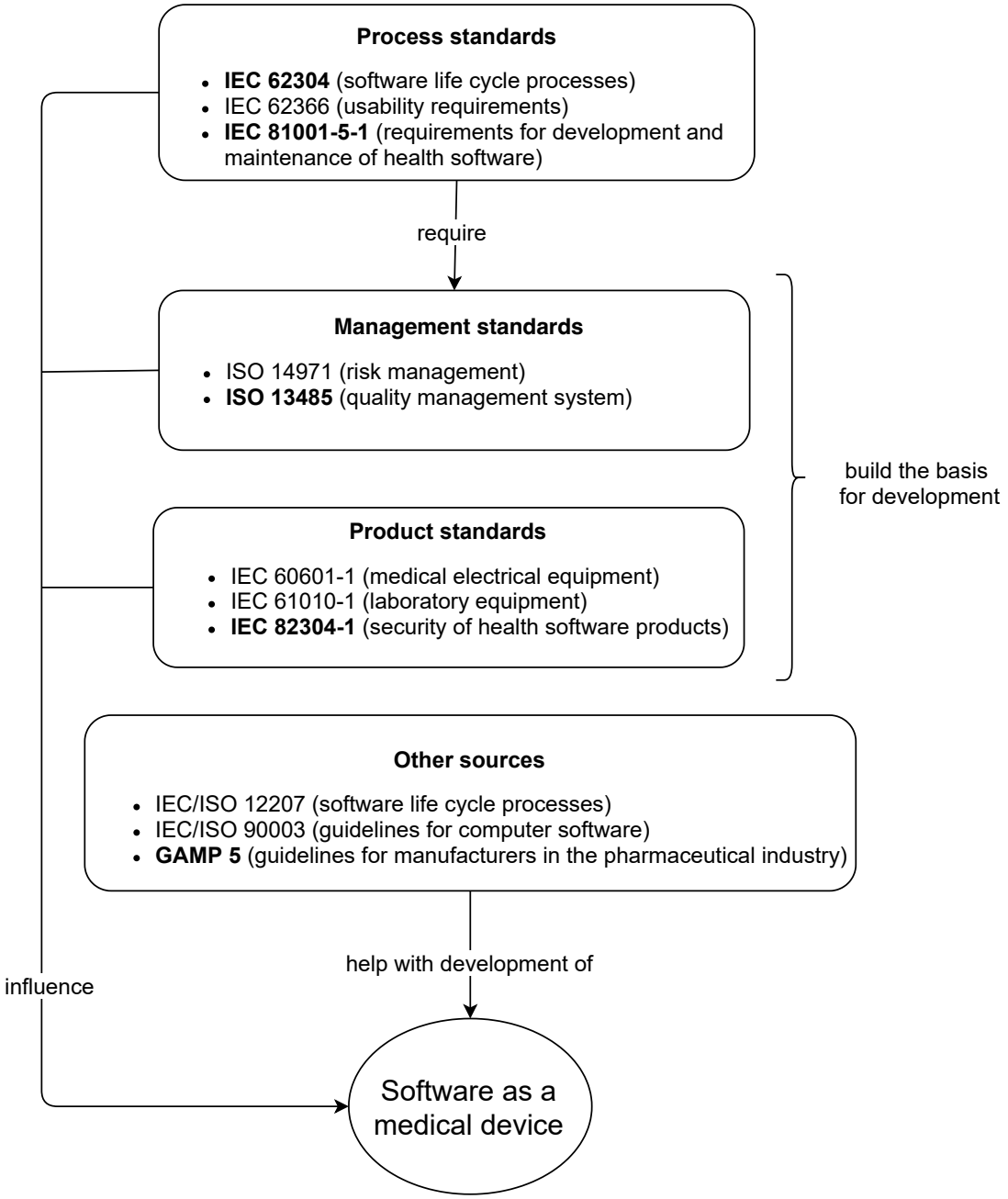


Figure 2.6: Relationship between standards for medical devices based on [35] and [19]

Several standards and norms related to medical devices have been published. The standards that were marked in bold are especially important when it comes to the development of health software. The standard IEC-82304 has only been published recently at the end of 2021 and manifests product requirements and software lifecycle processes compactly within 28 pages [19].

2.2.3 eSano as an eHealth platform of the University of Ulm

eSano is a platform that falls under the category of an eHealth system [4]. Different departments of the University of Ulm, such as the Department of Psychology and the Institute of Databases and Information Systems, started collaborating on this IT project in 2017. The idea was to create a system that allows gaining knowledge about mental and behavioral health. This has been achieved by creating three separate entities, i.e., a Content Management System (CMS), an eCoach platform, and a cross-platform application for participants. These interdependent entities rely on a single back end based on the REST[6] architecture and have been developed using different web development frameworks like Vue.js and Angular. eSano aims to provide a suitable and modern solution by allowing health care professionals to create internet- and mobile-based interventions, so-called IMIs. Interventions are measures taken by a therapist which are used to initiate solutions in order to prevent negative procedures (prevention) and to help people to recover from crises (rehabilitation) [36]. Users are guided by eCoaches when working on interventions [4]. Due to the importance of interventions, they have been developed in a way where therapists can add, remove or exchange modules on top of the standard configuration of the corresponding intervention. The progress of assigned modules can then be tracked by the responsible people, who stay in close contact with their patients.

We have summarized the functionality, the interdependencies between entities, and the considered regulations for the development of eSano in Figure 2.7.

[6] Representational State Transfer.

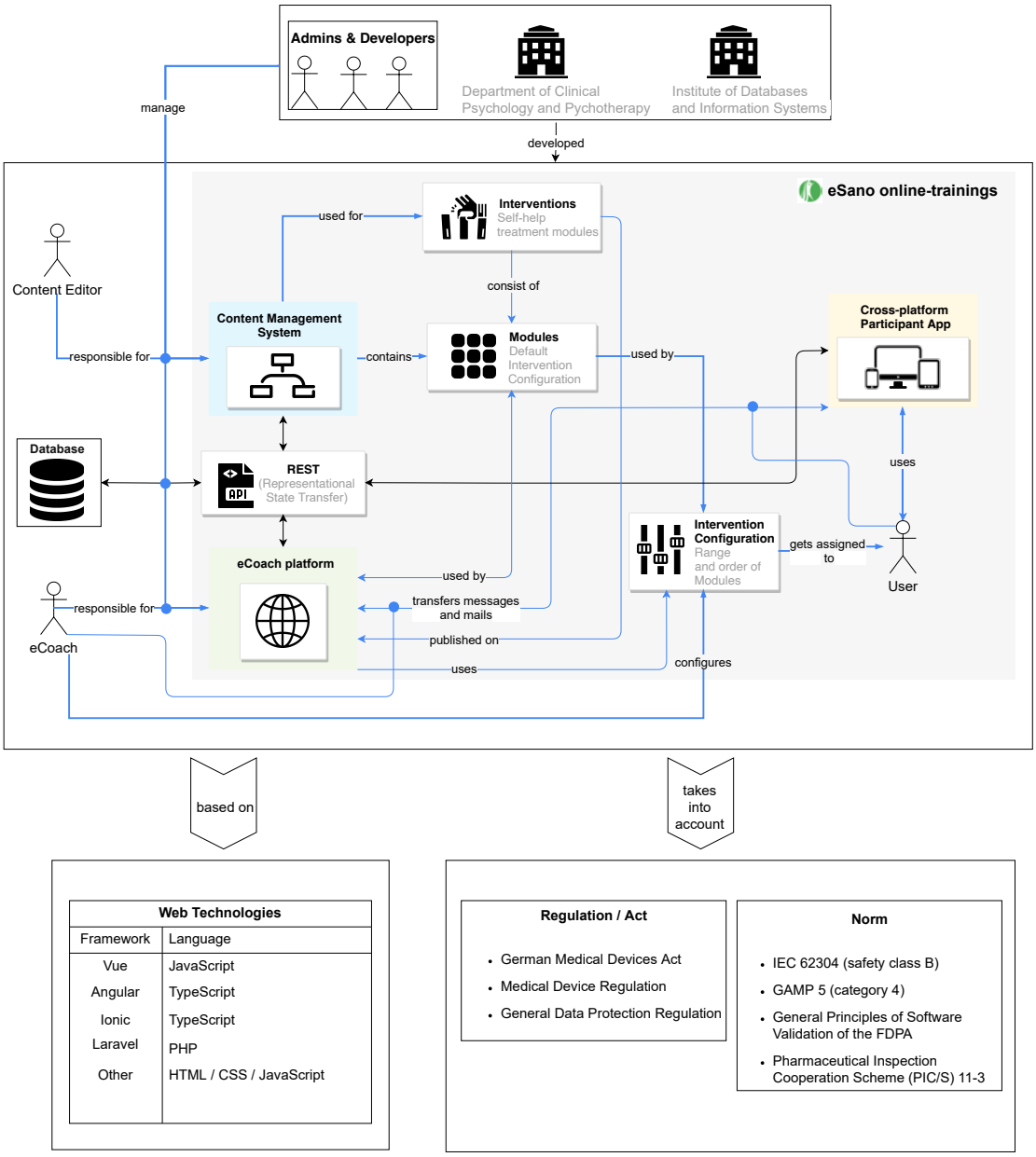


Figure 2.7: eSano's entities and their interactions based on [4]

The illustration depicts that multiple systems are used to provide users with modules on the web. Content editors are responsible for the CMS while specialists or eCoaches use the eCoach platform and mails to communicate with the user. We should note that the development of this platform considered several regulations and norms to ensure a high standard of security and to satisfy development standards, such as "Good Automated Manufacturing Practice"

(GAMP). It has been built using modern web development frameworks such as Vue.js and Angular.js and aims to add more features for future purposes. We will review the compliance of this platform with the GDPR in Section 4.2 and examine its front- and backend.

2.3 Summary

We started this chapter by noting that the history of data protection dates back 40 years and realizing that the territorial scope is an aspect hat should not be disregarded as each country follows its own rules for data exchange. Even countries like England or the US enacted health-related regulations that have similarities with the GDPR. We continued by elaborating each of the seven principles of the GDPR and looked at eHealth platforms in its context afterwards. Using Figure 2.7 we looked at eSano's components which we will examine in more detail during the application phase. In the following chapter, we will deep dive into the GDPR and how its articles work in practice.

3

The GDPR and its implementation in practice

In general, all companies should assess the extent to which they handle personal data per the GDPR, as violations can lead to heavy fines [9]. To avoid large fines, the GDPR explains that processing data is lawful if one has received permission from the user in Recital 40. The subsequent recitals, such as Recital 42 or 43, outline the details of consent which is a legal basis for the collection, processing, and use of personal data. Chapter 3 will summarize the GDPR, compare it with other legislation and outline best practices for companies.

3.1 Concise and succinct summary of the GDPR

The GDPR consists of eleven chapters which include 99 articles in total [9]. It is not necessary to inquire into every article to comply with the regulation. For health app providers, complying with regulations is difficult because other restrictions have to be considered as well. Interfaces with other regulations like the MDR or the FDPA are described in Section 3.2. We will only look at the most important key aspects of the GDPR.

3.1.1 Stakeholders

We have created a use case diagram in Figure 3.1 which depicts the interdependencies between the stakeholders of the GDPR.

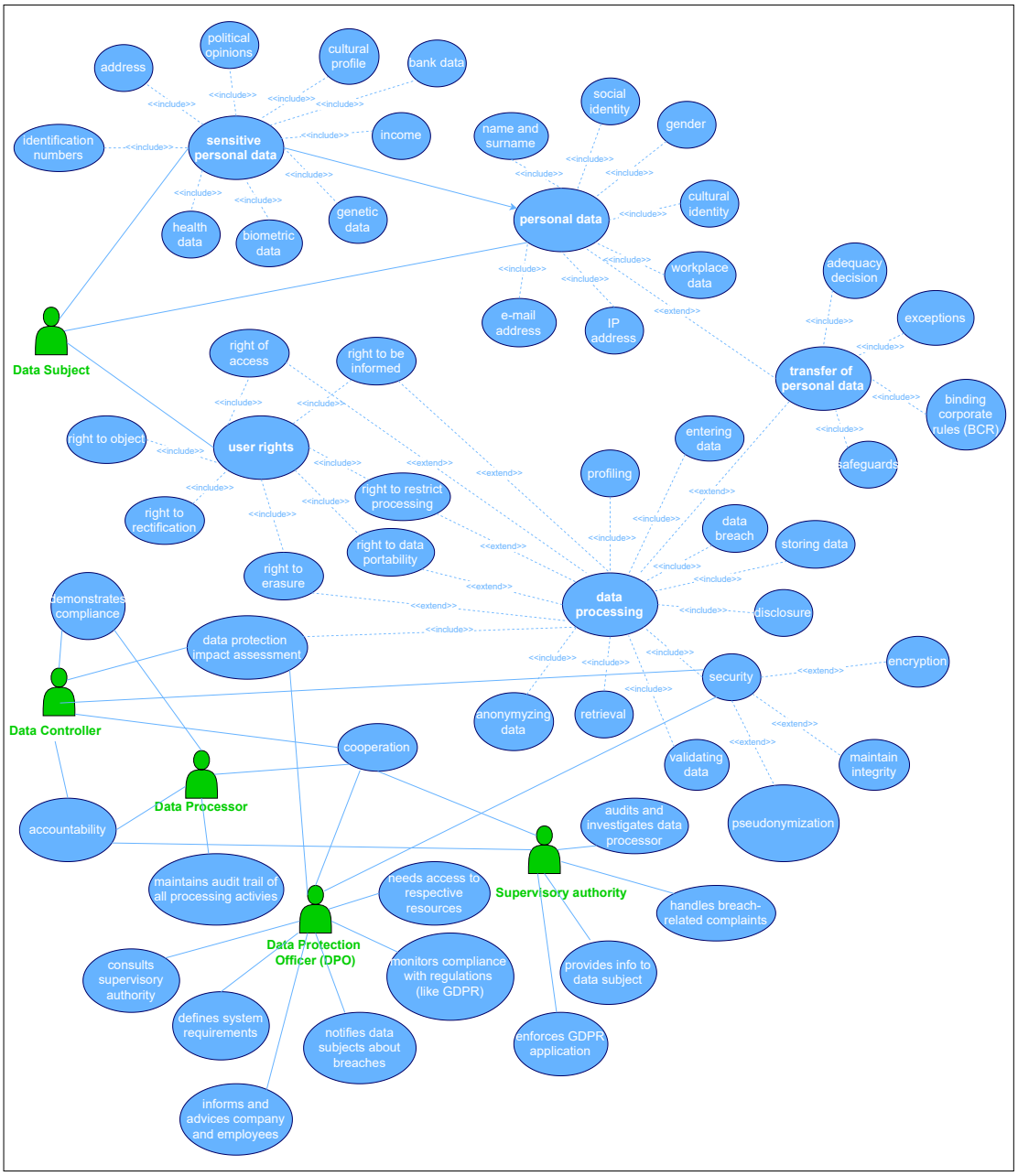


Figure 3.1: Use case diagram of stakeholders in the GDPR based on [37] and [38]

A data subject is a person living in a country of the EU, while a data controller is an institution, business, or person that determines how the data will be processed [9]. The data controller appoints a Data Protection Officer (DPO) who monitors the data protection practices according to Art. 13(1)(b) GDPR and

Art. 37(1) GDPR. The DPO also advises the data controller per Art. 35(2)(a) GDPR and Art. 39(1)(a) GDPR. A data processor is a company or institution that processes data on behalf of the controller while a supervisory authority monitors the implementation of regulations like the GDPR or MDR.

3.1.2 Consumer rights and possibilities

Art. 4(7) defines that the person or the agency responsible for data processing is the one who determines certain key elements, namely the purposes and means of data processing [9]. In other words, the controller decides on the why and the how of the processing.

In Chapter 3, it sets out the right

- to be informed
- of access
- to rectification
- to erasure
- to restrict processing
- to data portability
- to object

The scope of the right to information extends to all the personal data stored, including metadata according to Art. 15(1) of the GDPR [9]. If a data subject asks the data controller whether personal data of them is processed under Art. 13 of the GDPR, they have a right to information about this data. The data subject must initially be provided with information about the type, content, and purpose of the stored data. Upon request, the controller must also provide the data subject with information about the purpose of processing, the categories of personal data processed, the storage period, and the existence of a right to rectification, erasure, and restriction of personal data. Note that this information must be provided even before the initial processing. If a user makes use of this right, Art. 12(3) states that the responsible person or company should provide the data as soon as possible within one month. Information can be withheld if disclosure would the rights of third parties (e.g., personal rights or copyrights) are violated.

To make use of the right to access, users should first ask whether personal data relating to them exist at all. If this is the case, their specific right to information

extends to the categories of data stored, the origin and recipients of the data, and the purpose of processing [9]. The disclosure must also inform about the planned storage period (at least the criteria for determining it) and the data subjects' rights, as well as appropriate safeguards in case the data is being transferred to a third country.

The right to rectification allows the data subject to have inaccurate information corrected [9]. In addition to this, the data subject may also request the completion of missing data. To achieve this, the user must submit a request to the data controller, which is not bound to a specific form and can therefore also be made verbally. Recital 59 indicates that the controller should provide the option of submitting the request electronically. This applies in particular if the data itself is also processed electronically.

The right to erasure is also known as "the right to be forgotten" and the conditions under which companies must delete personal data are regulated in Art. 17 of the GDPR [9]. An obligation to delete may emerge, for example, if the data subject requests it, if they revoke a previously given consent, or if they object to the further processing of their data. However, there are also exceptions to the obligation to delete. There is no obligation to delete data if the processing is (still) necessary or if the processing of data serves a legitimate public task or the public interest. For instance, it does not have to be deleted if the data is used for historic, scientific, or health purposes. Other reasons are defined in Art. 17(3) GDPR.

The conflict between a deletion obligation and legally prescribed retention obligations is resolved via Art. 6(1) GDPR [9]. According to this, personal data may be stored if it fulfills a legal obligation of the controller. Legal retention obligations represent such a legal obligation and thus the legal basis for further processing. The user is entitled to request the processor to restrict their data for further processing. This does not mean the deletion of this data. Instead, it denotes that the personal information is marked so that the processing is not possible in its entirety.

The right to data portability in Art. 20 of the GDPR gives the individual the possibility to receive data stored about them in a portable format or, if applicable, to transfer the data directly to the other provider [9]. It gives the person the the possibility of transferring the data stored about him or her (e.g., on social media) in a suitable portable format or, where appropriate, to transmit the data directly to another provider.

Art. 21 defines when users can object to processing their data [9]. Suppose the person uses their right to object, and their data is used for direct advertising and associated profiling. In that case, the objection does not have to be justified, and

the responsible entity is not allowed to use it anymore. If the processing is for purposes other than direct advertising, one must provide a plausible reason for the objection. Whether the company still processes the data depends on the individual case, e.g., if the processing serves to exercise or defend legal claims. If the processed data is used for scientific purposes, the individual can subject unless the processing is done due to public interest.

3.1.3 Data Protection Management

A Data Protection Management System (DPMS) defines how personal data is to be handled in companies [39]. It is an internal guideline based on the GDPR and it helps to manage and monitor internal data protection. The GDPR does not mandate a DPMS explicitly. However, the legal requirements for the operation of a DPMS can be derived from some articles and recitals. Through an up-to-date DPMS, employees and responsible parties have a guideline that they can follow to guarantee the correct and secure processing of personal data. This has to be ensured legally, technically as well as organizationally. Recital 78 of the GDPR requires the controller to have internal strategies to demonstrate compliance with the regulation [9]. In the event of an inspection by authorities or supervisory procedures, the company's internal data protection can be concretely demonstrated, and the threat of a fine can be mitigated or prevented according to Art. 83(2) GDPR.

Different ISO management systems follow the principle of the Plan, Do, Check and Act (PDCA). The PDCA cycle is the response to an environment that is constantly changed by factors such as market, competition, and legal framework. It consists of four phases, and we have described their context within the GDPR in Figure 3.2.

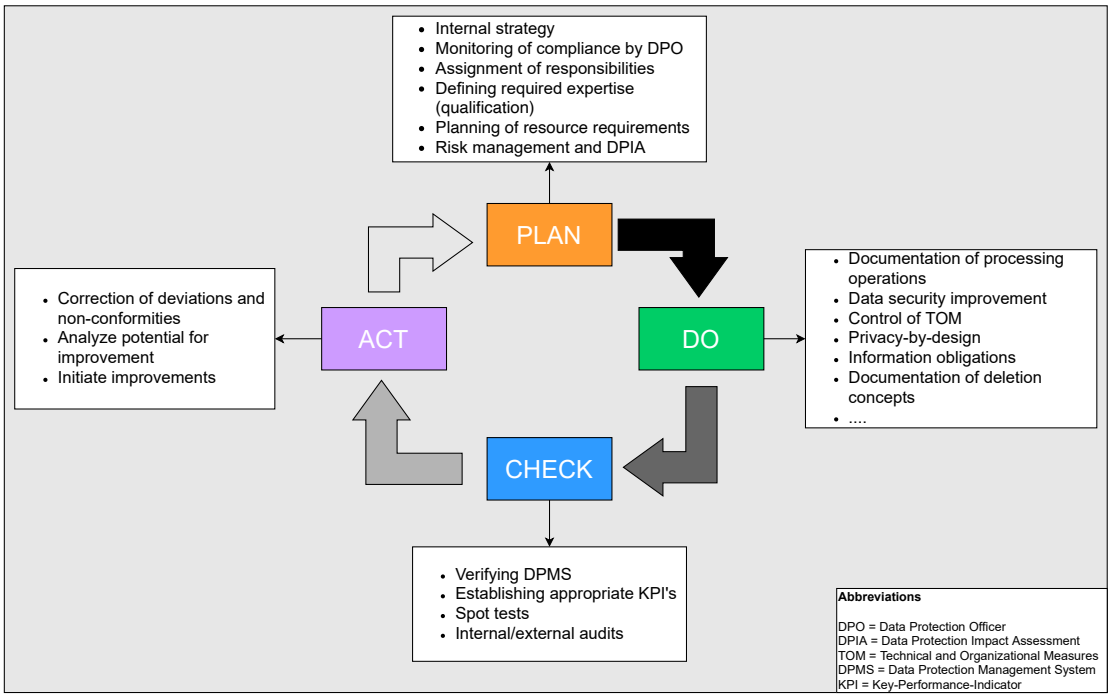


Figure 3.2: PDCA cycle in the context of GDPR based on [9] and [39]

While we have manifested the core functionalities of a DPMS in the figure above, we have not yet referred to the corresponding articles of the GDPR. This will be done in Section 3.2.

Art. 32 of the GDPR postulates that the controller and processor have to take appropriate TOM to guarantee data security and to reduce the risk of data misuse [9]. The term TOM already indicates that the measures can be technical and organizational. Technical measures include physical procedures, such as protecting the company building with a lock. An organizational measure, in this case, would be to document the distribution of keys. The GDPR specifies that the level of protection should be adapted to the respective risk and that various measures should be included in it. According to Art. 32(1) of the GDPR, the actions taken should consist of the following points:

- pseudonymization and encryption
- confidentiality, integrity, availability, and resilience of processing systems
- data recovery
- testing, assessing and evaluating the effectiveness of TOM

Per Art. 4(5) GDPR, pseudonymization means that the processing of personal data has to be designed so that a reference to a user is only possible with additional information that must be kept separately and must be protected from access by unauthorized persons by TOM [9]. Therefore, it is important to note that it is still possible to identify a person by merging data. That is why some provisions of the GDPR continue to apply. For example, if the legal retention obligation expires and other retention reasons are missing, pseudonymized data must also be deleted. The advantages and possibilities of pseudonymization and encryption will be explained in Section 3.2.

Encryption is not mandatory under the GDPR, but Recital 83 of the GDPR states that encryption offers a suitable solution to maintain security [9]. The most common data encryption methods are asymmetric and symmetric encryption [40].

Examples of asymmetric encryption are:

- SSH: Secure Shell (SSH) refers to a protocol through which appropriate programs (clients) can access a remote computer and execute commands or actions on it [40].
- SSL/TLS: SSL stands for “Secure Socket Layer”, TLS for “Transport Layer Security” and they are both cryptographic protocols that encrypt data and authenticate a connection when data moves across the internet [40].

Examples of symmetric encryption are described in the list below.

- 3DES: DES stands for Data Encryption Standard and uses a key length of 56 bits. Triple DES uses a key length of 168 bits, which is three times as long, hence the name [41].
- AES: AES (Advanced Encryption Standard) is used to secure and encrypt operating systems, hard drives, network systems, files, emails, and similar data [41].
- RSA: RSA (Rivest–Shamir–Adleman) is a system for encryption and authentication and is considered the most widely used algorithm for encryption and authentication [41].

Strictly speaking, the term “anonymization” is not to be found in the legal text of the GDPR; it is only explicitly mentioned once in Recital 26 of the GDPR [9]. When data is anonymized, the personal reference is completely removed, and there is no additional information. Technically, this is implemented, for example, by algorithms that transform names into codes using a random mechanism (randomization). Without personal reference, anonymized data no longer falls within the scope of the GDPR.

Figure 3.3 portrays the difference between both.

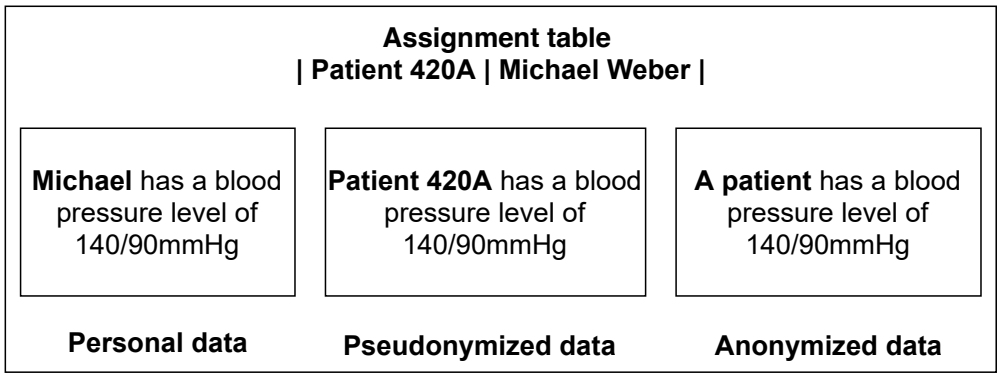


Figure 3.3: Difference between pseudonymization and anonymization based on [42]

The concept of integrity refers to the completeness and accuracy of the processed data and the processing operation [9]. Unauthorized modification of the data is prohibited. At the same time, a correction must be made if data has been processed incorrectly. To ensure integrity, electronic signatures, check digits, input controls, or authorization systems may be required for access. Availability refers to the accessibility of processed data. However, storage limitations are also needed, and data must be deleted at regular intervals when it is no longer needed for the intended purpose.

A suitable and appropriate level of protection must be maintained permanently [9]. Since the actual and legal circumstances of the TOM change regularly, it is vital to conduct periodic reviews, and to assess and evaluate measures critically. For instance, the cybersecurity standard IEC 81001-5-1 was published in December 2021 [43]. It includes medical devices and other software used in healthcare and considers stakeholders, such as healthcare providers. Another protective measure for data security is listed in Art. 32(4) GDPR, which states that persons who have access to personal data may only act on the instructions of the controller or processor [9].

3.1.4 Data Protection Impact Assessment

Providers of eHealth apps must conduct a Data Protection Impact Assessment (DPIA) as the processing and storage of personal information involves a high

risk [44]. The Standard Data Protection Model (SPM)[1] or ISO standards can be used as methods for the DPIA. When it comes to the development of health software, there are different IEC and ISO standards. Regardless of this, however, the DPIA must include specific minimum requirements by Art. 25(7) of the GDPR [9]. A summary of these requirements can be found in phase one of the DPIA in Figure 3.4.

If one cannot assess when an exceptionally high risk exists, one can look at Art. 35(3) of the GDPR which defines when a DPIA is necessary [9]. Examples include profiling, processing the kind of personal data described in Art. 9(1), or extensive surveillance of public areas. These examples are not very specific, so determining the necessity of a DPIA often causes difficulties [44]. Here, however, the European legislator has imposed an obligation on the respective State Data Protection Officer in Art. 35(4) GDPR to provide further specifics on so-called "positive lists" [2].

Based on the handbook for DPIA in the context of Art. 35 of the GDPR, we have illustrated the process in Figure 3.4.

[1] The SPM is a procedure that can be used to translate the legal requirements from the GDPR into concrete TOM. It is developed by a sub-working group of the Data Protection Conference.
[2] They include processing activities where a DPIA must definitely be carried out.

Figure 3.4: DPIA procedure in the context of Art. 35 of the GDPR based on [44]

As seen in Figure 3.4, a DPIA consists of five phases [44]. The approach for each phase has been packed for the sake of length of this thesis. The initial screening serves the purpose of assessing the risk of processing personal data. In the second phase, documentation is being focused upon. The third and fourth phase consists of the identification and implementation of measures. In the last step, the impact and effectiveness of the DPIA must observed. Apart from that, a DPIA is not required according to Recital 91 of the GDPR, if only a single individual, e.g., a health professional, processes data on a small scale [9].

3.1.5 Lawfulness of data processing

Before an external service provider can be commissioned to process personal data (order processing), the client and contractor must first conclude a written contract [9]. Art. 28 of the GDPR specifies what this contract must contain. Every data controller and data processor must create and maintain a Record of Processing Activities (ROPA) involving personal data according to Art. 30 of the GDPR. The inventory of processing activities serves as an essential basis for the CCPA. It helps the controller to demonstrate compliance with the requirements of the GDPR in accordance with Art. 5(2) of the GDPR, i.e., accountability.

Recital 54 of the GDPR states that processing sensitive health-related data might “be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures to protect the rights and freedoms of natural persons” [9, Recital 54]. Processing this kind of data must not eventuate in other uninvolved parties, e.g., insurance companies, using the data according to Recital 53. Nonetheless, this should not exacerbate data transfer within the EU, which implies that the EU tries to unify data protection legislations.

The GDPR regulates the possibility of imposing fines by the respective competent DPA in Art. 83 if data is processed unlawfully [9]. The article contains criteria considered by DPA’s when assessing a fine. These include, for example, the type, the severity, and the duration of an infringement, as well as the intentionality in causing it. The data protection authorities determine fines according to the law based on these criteria. The maximum amount of a fine can be up to 20 million euros or four percent of a company’s annual global turnover, whichever is higher. To transfer (personal) data to a country outside the EU, it is a prerequisite to check whether the transfer complies with Art. 28 of the GDPR [34]. If so, the respective company or institution must verify whether Art. 44 et seq. GDPR are fulfilled, or not.

3.2 Interfaces with other regulations

The enactment of the GDPR in 2018 updated the Data Protection Directive 95/46/EC of 1995 by resolving uncertainties and therefore providing a neutral framework for data protection [45]. The GDPR allows its member states to complement or modify the GDPR with so-called “opening clauses” that would enable national legislators to regulate certain matters in deviation from the GDPR and to specify them for the member state [9]. Federal laws, such as the FDPA, cannot differ in the principles of the GDPR because European law takes precedence over federal law [12].

3.2.1 Differences between Data Protection Directive 95/46/EC and the GDPR

The DPD aimed for consistent data protection rules in the EU [30]. In its second article, it defined eight terms, such as “personal data” and “processor” [46], whereas the GDPR added new words in Art. 4, such as “data concerning health” or “binding corporate rules” [9]. When the DPD was still in effect, data controllers had to inform supervisory authorities before data processing could take place [30]. As of the introduction of the GDPR, specifically Art. 30, this is not necessary anymore. Instead, the responsible entity for data processing has to provide the supervisory authority with a Records of Processing Activities (ROPA) [9].

The Article 29 Working Party is an advisory council formed under Art. 29 of the DPD and includes supervisory authorities of the EU member states and a representative of the European Commission [46]. It was dedicated to data protection until the GDPR got enforced. The Working Party noted that data processing for research was legitimate if the data controller used adequate safeguards. Art. 35(2)(a) of the GDPR requires data controllers to do a DPIA, which is a safeguard as well [9]. The GDPR does not ask for consent for further data processing, whereas health-related user data could only be further processed under the DPD if the data subject consented to it [46]. Also, Art. 5(1)(b) of the GDPR defines the aspect of purpose limitation [9], while the Working Party considered purposes to be “specific”, “explicit”, and “legitimate” [46].

Due to changes in technology, the GDPR needed to adapt the definition of personal data. A specific example of how the GDPR incorporated a broader definition of that term can be seen in Table 3.1.

DPD and GDPR	
Law	Personal Data
DPD	• Name • Address • Photo • E-Mail • Personal Identification Numbers
GDPR	• Name • Address • Photo • E-Mail • Personal Identification Numbers • Biometric/Genetic/Health data • Cultural/Social Identity • IP Addresses • . . .

Table 3.1: Comparison of personal data in the DPD and GDPR based on [9] and [46]

The DPD did not define how data processors must be regulated [46]. Thus, it was always the data controller who was responsible for everything. Under the GDPR, data processors can also be prosecuted, which is why a DPO has to inspect the main activities of an organization [9]. Art. 30 of the GDPR states that companies and institutions with more than 250 employees do not need documentation of introduced data protection policies unless the processing includes special categories of personal data.

Art. 33 of the GDPR also requires a data controller to inform a supervisory authority within 72 hours of a breach [9]. Contrary to this, the DPD referred to the adoption of data breach notification laws, where the organization had to comply with their respective state laws in the event of a breach [46]. Each member state decided the range of penalties in case of violations, and it was uncommon for companies to pay fines under the DPD. Other, more general changes are that (explicit) consent requires users to confirm to data processing and that companies have to delete data which does not serve its primordial purpose.

3.2.2 Federal Data Protection Act

The (new) FDPA came into force simultaneously as the GDPR on May 25, 2018 [47]. From a territorial perspective, the FDPA applies to data controllers and processors who process personal data in Germany or within the scope of the activities of a German business as defined in Section 1(4) of the FDPA. In the following, we will always refer to the new FDPA.

An area of regulation that the GDPR entrusts to the FDPA is processing personal data by public authorities [47]. For the health sector, Art. 9(2)(h) of the GDPR [9] applies in conjunction with Section 22(1) of the FDPA which permits processing of special types of personal data for preventive health care or treatment in the health or social sector [47]. All data processing operations in connection with prevention, diagnostics, therapy, and aftercare are thus permitted.

While Art. 37 of the GDPR states that the processing of special categories of personal data, such as health data, require a DPO [9], Section 38 of the FDPA provides three conditions for the designation of a DPO for non-public bodies [12]:

1. 20 people are involved in the processing of personal data
2. A DPIA is mandatory
3. The data processor handles data for (anonymous) transmission or market research

Since the usage of Excel lists are already considered automated data processing, the DPO designation obligation practically exists for all healthcare-related companies with more than 20 employees [31]. Art. 39 of the GDPR presents that the DPO is responsible for monitoring compliance with the GDPR and should act as a contact person for supervisory authorities and data subjects [9]. Due to the sensitivity of the data and the variation in legal sources, a DPO in the

healthcare sector should also have medical knowledge appropriate to the area of responsibility.

Art. 88 of the GDPR provides the option of regulating employee data at the national level [9]. Germany made use of this in Section 26 of the FDPA. It defined that employers may process such personal data that is necessary for the performance, termination, or commencement of an employment relationship even without the employees' consent [47].

While Art. 13 and 14 of the GDPR contain information obligations that need to be fulfilled by data processors [9], Section 32 and 33 of the FDPA tell us that users do not have to be informed about data processing in certain cases, e.g., public security or if "the controller's interests in not providing the information outweigh the interests of the data subject" [47, Section 32(1)].

If personal data are processed for the purposes of automated evaluations, this is referred to as profiling according to Art. 4(4) of the GDPR [9]. Following Art. 22 of the GDPR, it is not the creation of user profiles itself that is problematic, but rather the use of these profiles. Recital 71(1) of the GDPR defines the term "Profiling" and clarifies that personal information, such as income level, must be used to exclude a user from a contract. Such profiling may be permitted under certain circumstances, provided that a law (following the direction of the EU Member States) specifically authorizes it or the user has given his consent. In Germany, the legislator regulated the permissibility of automated decision-making based on the processing of health data at national insurance companies in Section 37(2) of the FDPA. Besides, if a user requests to stop profiling pursuant to Art. 19 GDPR, the processing must stop [47].

In addition, the user's right to access per Art. 15 of the GDPR does not apply if the data is required for scientific research, and the provision of information would require disproportionate effort [9]. Section 29(1) of the FDPA states that information does not have to be provided if it discloses intelligence that must be kept secret according to a legal provision [47]. This includes information that is subject to medical confidentiality, and thus, information that affects third parties. Persons whose profession swears them to secrecy, such as physicians or counselors, are granted an exception to investigative powers according to Section 29(3) of the FDPA, which is generally described in Art. 58 of the GDPR [9].

Also, Sections 32 and 33 of the FDPA provide further exceptions to information requirements [47]. For instance, according to Section 32(1) FDPA, the obligation to provide information under Art. 13 GDPR shall not apply if the enforcement or defense of legal claims would be impaired and the interests of the controller in not providing the information outweigh the interests of the user [9].

In case of severe violations of the GDPR, Art. 83(5) imposes fines of up to 20 million euros or four percent of the global revenue of a company if it is higher [9]. In contrast to that, Art. 43(2) of the FDPA states that the violation of the right to information and the failure to inform users seasonably could lead to a maximum fine of 50,000 euros [47].

3.2.3 Medical Device Regulation

The Regulation (EU) 2017/745 for medical devices, otherwise known as the Medical Device Regulation was published in 2017 and has been mandatory since May 2021, after a four-year transition period [20].

The MDR is based on:

- the Medical Devices Directive 93/42/EEC
- the Active Implantable Medical Device Directive 90/385/EWG

The MDR differentiates between four risk classes: I, IIa, IIb, and III [48]. The higher the classification, the higher the risk, and the more invasive the product. Rule 11 of the Annex VIII of the MDR states that software “intended to provide information which is used to make decisions with diagnosis or therapeutic purposes is classified as class IIa [. . .]” [48, Section 6.3 MDR] except of serious injuries (IIb) and death (III). Everything else can be assigned to class I. If software is classified at least as class IIa, it requires regulations such as a certified Quality Management System (QMS) (EN ISO 13485) and TOM [49]. Figure 3.5 provides a short overview of how to classify software based on rule eleven of the MDR.

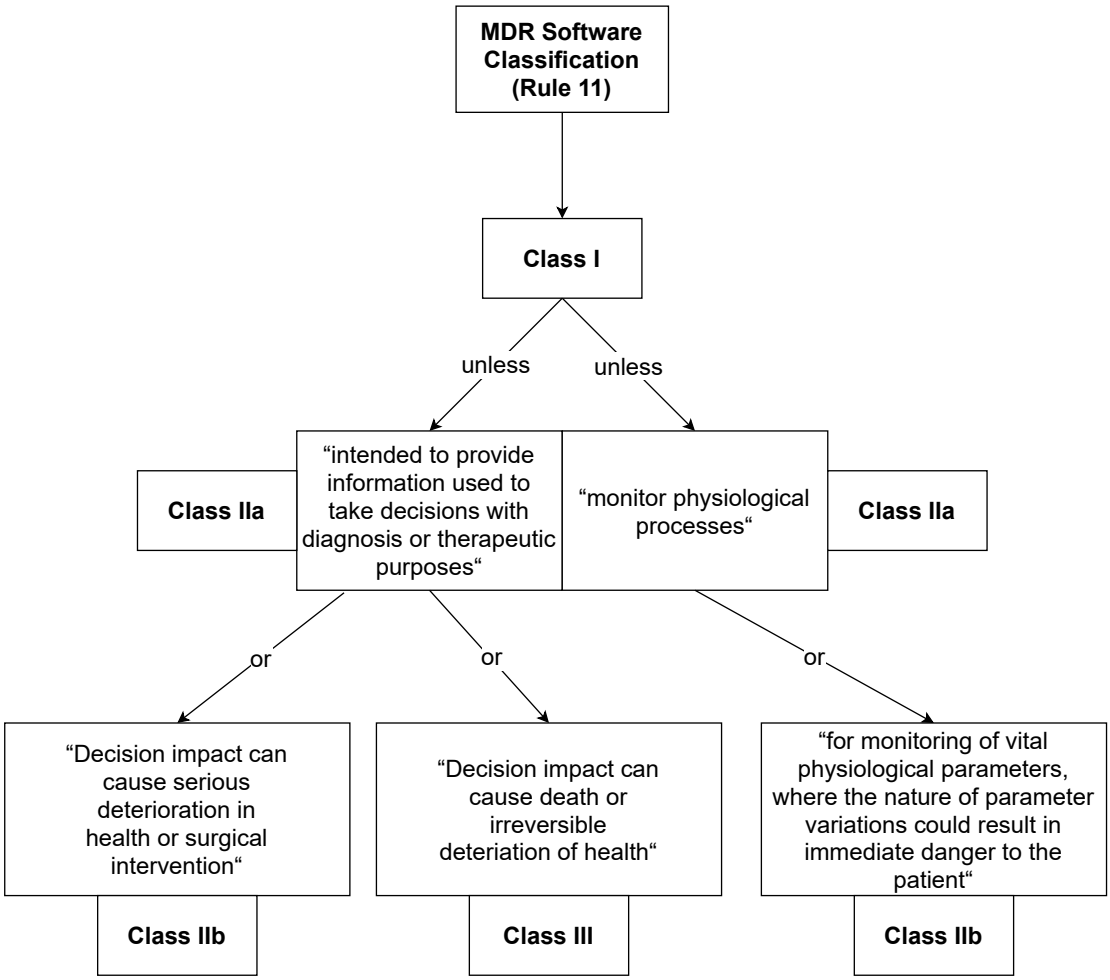


Figure 3.5: Risk classification based on [50]

The Medical Device Coordination Group (MDCG) noted that almost all software has to be classified as class IIa at the minimum [50]. In the worst case, something terrible can always happen, resulting in a lot of class III software. The MDCG created a table that is based on classifications by the International Medical Device Regulators Forum (IMDRF) and facilitates the process of classifying lower than class III.

To harmonize different norms, the IMDRF published a guideline for (health) software developers [51]. Figure 3.6 summarizes it.

Figure 3.6: Guidance for medical device software to comply with ISO 13485 based on [51]

As shown in Figure 3.6, we distinguish the requirements in three areas: activities, organizing, and processes. Activities include responsibilities, for instance, the

implementation of risk control measures. Processes are about the development planning, among others, while the requirement to organize requires the introduction of a QMS. The IMDRF is a voluntary association of authorities who have the task of approving medical devices and software in their countries [51]. Together, they strive for harmonized rules and create guidelines to help companies to comply with norms like ISO 13485. However, one should note that the IMDRF guideline(s) do not cover many aspects of the standard ISO 13485, such as measurement tools for software developers. It should, therefore, rather be used to gain valuable insights. Figure 3.6 can build the basis for whether a company should aim for complying with ISO 13485 or not. We will look at other important norms in Section 3.2.5.

3.2.4 Similarities and differences between GDPR and MDR

Producers of medical devices can be considered data controllers and processors according to Art. 4(7-8) [9]. Therefore, they must always conduct a DPIA to handle clinical data. Per Art. 61(2) MDR, companies must inform an expert if their medical device is classified in class IIb or III to examine whether the device can be used for clinical purposes [48]. This is akin to Art. 37 GDPR, where a DPO must be designated who ensures that a business complies with the law [9].

As outlined in Section 2.1.3, the term “confidentiality” in Art. 5(1)(f) represents one of the key principles of the GDPR [9]. The MDR states that data records must be handled confidentially, and that personal user data should be protected based on the law that applies with regard to data protection in Art. 72(3) [48]. We can see that the MDR does not explicitly mention the GDPR in this context because other laws may apply as well.

Just as Art. 24 GDPR outlines the responsibilities of a data controller [9], Art. 15 MDR defines responsibilities of the person in charge of compliance [48]. The responsible party must be registered in EUDAMED, the European Database on Medical Devices [52]. Figure 3.7 summarizes responsibilities in the context of the MDR.

Article 15(3) (Person responsible for regulatory compliance)	**MDR-related articles/appendixes**	**Content**
Conformity of device in the context of a QMS	Art. 10(9)	Establish/document/implement/maintain/ (continually) improve a QMS that has to ensure compliance with the MDR
Technical documentation	Art. 10(4) Annex II Annex III	Technical documentation that includes: - description of device and operation instructions - list of configurations - functionalities and diagrams/pictures that help with understanding
EU declaration of conformity	Art. 10(6) Art. 19 Annex IV	Declaration of conformity per Art. 19-20 MDR that contains the info laid out in Annex IV
CE marking	Art. 20 Annex V.	CE marking that should be put onto the device
Post-market-surveillance obligations per Art. 10(10) MDR	Art. 10(10) Art. 83	Post-market surveillance system per Art. 83, that includes: - data based on quality, performance and safety of device - determine/implement/monitor preventive actions
Obligations according to Art. 87 and 91 MDR (Post-market surveillance plan + implementing acts)	Art. 10(13) Art. 87 Art. 88 Art. 89 Art. 90 Art. 91	- System of recording and reporting incidents per Art. 87-88 MDR - Incidents related to devices on the market must be reported per Art. 88 MDR - Serious public health threats must be reported immediately and not later than two days after awareness

Figure 3.7: Responsibilities of the person in charge of compliance in the context of the MDR based on [52] and [48]

When looking at the content column of Figure 3.7, we can see that it overlaps a lot with the responsibilities a data controller needs to take care of for the GDPR. For instance, under certain conditions, the GDPR requires documentation such as records of processing activities, TOM, or a DPIA [9]. If an organization is GDPR-compliant, it will, by default, have most of the documents available necessary to comply with the MDR as well.

Art. 109 of the MDR states that entities which have to comply with the MDR must consider the secrecy of data that is being worked with [48]. Compared to that, the GDPR outlines confidentiality as one of its basic principles in Art. 5. The similarity is that the MDR and GDPR have loose definitions of what kind of measures companies should take in this regard.

Art. 110, which is intended to describe data protection, only refers to two outdated legislations, i.e., the DPD and Regulation No 45/2001. Nevertheless, if an application is a medical device that collects personal data, it will always be subject to the GDPR. Therefore, the practices described in Section 3.3 should be actioned. Art. 42(3) of the GDPR states that it does not need certification [9], whereas a medical device (apart from class I) has to be certified by a notified body according to the MDR [48].

Companies can put a Conformité Européenne (CE) mark on their medical device if it passes a conformity assessment exerted by an EU authority [53]. The mdc medical device certification company in Germany described which requirements have to be fulfilled to get the CE certification [54]. As for software verification, the software lifecycle and design have to be described. Software validation and usability tests are also required. Further, software should also be identifiable with a Unique Device Identification.

3.2.5 Other relevant standards and their relationship with the GDPR

The norm DIN CEN ISO/TS 14265 classifies what kind of health data can be processed [55]. This is necessary given that Art. 25(1) of the GDPR requires that the grounds for processing personal data must be taken into account [9].

In general, Section 630(f) of the German Civil Code (GCC) prescribes a retention period of ten years for patient records unless more specific laws dictate otherwise [56]. Even before the GDPR came into force, Section 630(g) of the GCC gave patients the option to inspect their patient records on request. This regulation is now extended by the right to information from the GDPR in Art. 15 [9]. Nonetheless, an inspection of the patient records can be denied if there are therapeutic reasons for not doing so: this is mainly the case if the patient file contains psychotherapeutic treatments and the patient could suffer harm from knowledge of the information contained therein [56].

Art. 42 of the GDPR calls for the introduction of a certification that attests the company's compliance with data protection requirements. The ISO/IEC 27001 Information Security Management Systems (ISMS) is a best practice framework

that helps companies to manage their information security risks, including those related to the protection of personal data [57]. It requires that they demonstrably know and appropriately comply with legal obligations, such as those arising from the EU GDPR. In addition, ISO/IEC 27001 contains security design and accountability requirements. If a company produces and runs a medical device, the ISO 27001 becomes especially important as the company is responsible for both, protecting the data and preventing the release of unsafe products [58]. We have summarized some compliance requirements for organizations depending on their role.

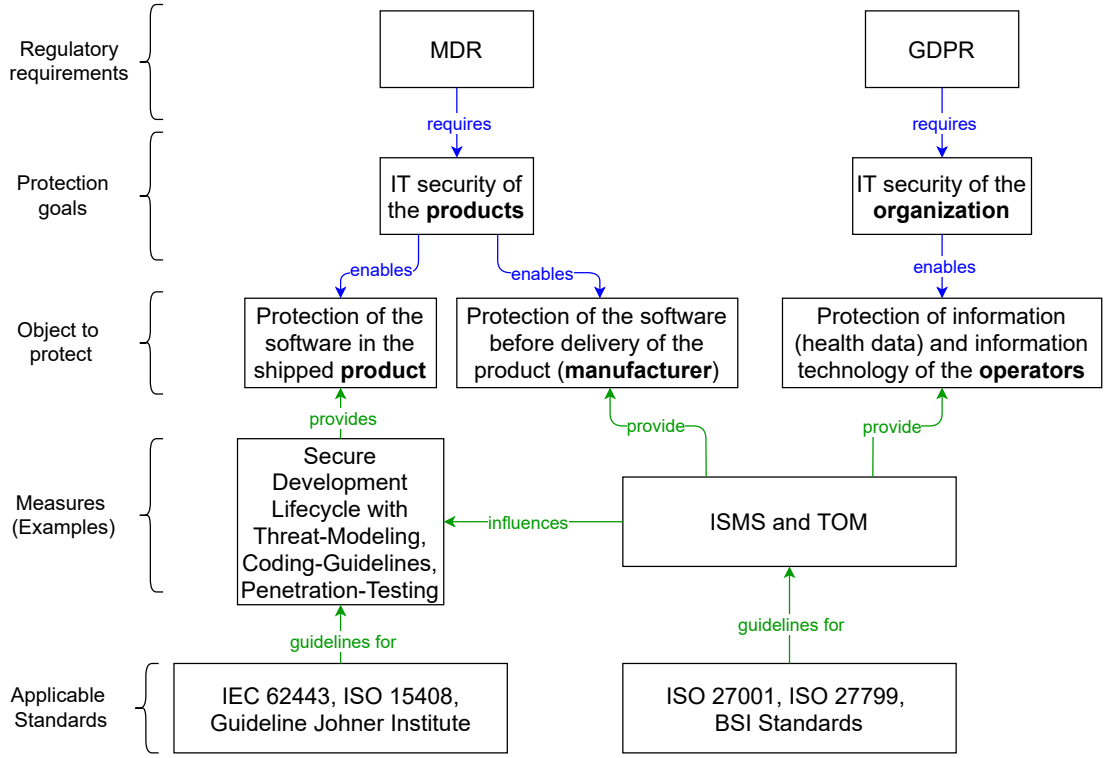


Figure 3.8: Summary of requirements depending on role of the actor based on [58]

Figure 3.8 shows that different standards can be applied depending on the role of the company. For instance, if a company is a manufacturer of a product and also operates it, they should use standards like ISO 27001 which can be used as a guideline for the implementation of ISMS and TOM. The Johner Institute explicitly says that the introduction of an ISMS per ISO 27001 is not too difficult and suggests companies processing health data to follow it [58].

3.3 GDPR-related best practices

The European Data Protection Board (EDPB) regularly publishes guidelines to improve the comprehension of the GDPR [59]. More than half a decade after the GDPR came into force, it is still not apparent how the new requirements can be met in practice in numerous instances. The guidelines and the practice of the data protection supervisory authorities are often only of limited practical use. At the same time, the German supervisory authorities are increasingly imposing hefty fines and carrying out more checks. With an ever-increasing number of legislation, especially health software development, it is indispensable to follow best practices. In the following, we will outline some of the best practices on what companies or healthcare institutions can do to comply with the GDPR.

3.3.1 Measures to prove compliance regarding data processing

Table 3.2 describes which measures institutions can take to fulfill the requirements of the GDPR stated in article five.

GDPR	
Article	Measures

5(1)(a) (Lawfulness)	• The purpose of use and the legal basis are presented in the ROPA and communicated to the data subject when data is collected. • The privacy policy shows how data protection is ensured in the company/institution. • The authorization concept specifies who is allowed to process data and the reasons for doing so. • A protocolling can check when someone has accessed data. • The data subject is given the option to object to any processing insofar as an objection is legally possible. • Establishment of a SPoC for users in case of questions.
5(1)(b) (Purpose limitation)	• Documentation of processing purposes. • Description of all processing operations, including the types of data that are necessary to meet processing objectives. • Auditing of the processing.
5(1)(c) (Data minimization)	• Documentation of processing objectives and proof that collected data are necessary to achieve the purpose. • Categorization of data.

5(1)(d) (Accuracy)	• Direct survey of the end user. • Use of hash values and electronic signatures to prove changes. • 4-eyes principle during data collection and processing.
5(1)(e) (Storage limitation)	• Earliest possible anonymization/deletion of data. • Blocking of data access if legally required storage exceeds the purpose for which data was collected. • Defining a maximum required storage period.
5(1)(f) (Integrity)	• Use of encryption such as hard disk encryption and database encryption. • Usage of hash values and electronic signatures to detect modifications. • Regular backups. • Redundant systems[3]. • System alerts when changing for sensitive data, e.g., “Do you really want to do this?”.
5(2) (Accountability)	• To prove that the data controller complies with the requirements of the GDPR, a documentation of all corresponding processes is required.

Table 3.2: Best-practices with regard to Art. 5 of the GDPR based on [60]

[3] Alternative systems or servers to increase reliability in case of failures.

In Section 2.1.3, we have described that data protection by design ensures transparency. This concept is familiar within the frame of scientific research as it proves compliance and is usually considered a prerequisite to receiving funding [45].

One should also note that state and federal laws do not only exist for health-related data [61]. In fact, there are archive laws that regulate what kind of documents and data can be archived. Premises can be that data has long-term values for research or if that it contains information relevant for legislation.

3.3.2 Privacy Policy

It follows from Art. 12 and Art. 13 GDPR that network addresses are personal data, so privacy policies on websites are mandatory. The data protection declaration should provide the user with comprehensive information about the storage and processing of their data and about the transfer of data to third parties. It should inform the user already at the beginning of the use, for example, before downloading an app. These rules are also critical for eHealth applications. The more precise and comprehensive the consent is formulated, the broader the possibilities for working with that data.

Art. 13 of the General Data Protection Regulation provides information about what kind of information privacy policies need to contain. Figure 3.9 provides an overview of that.

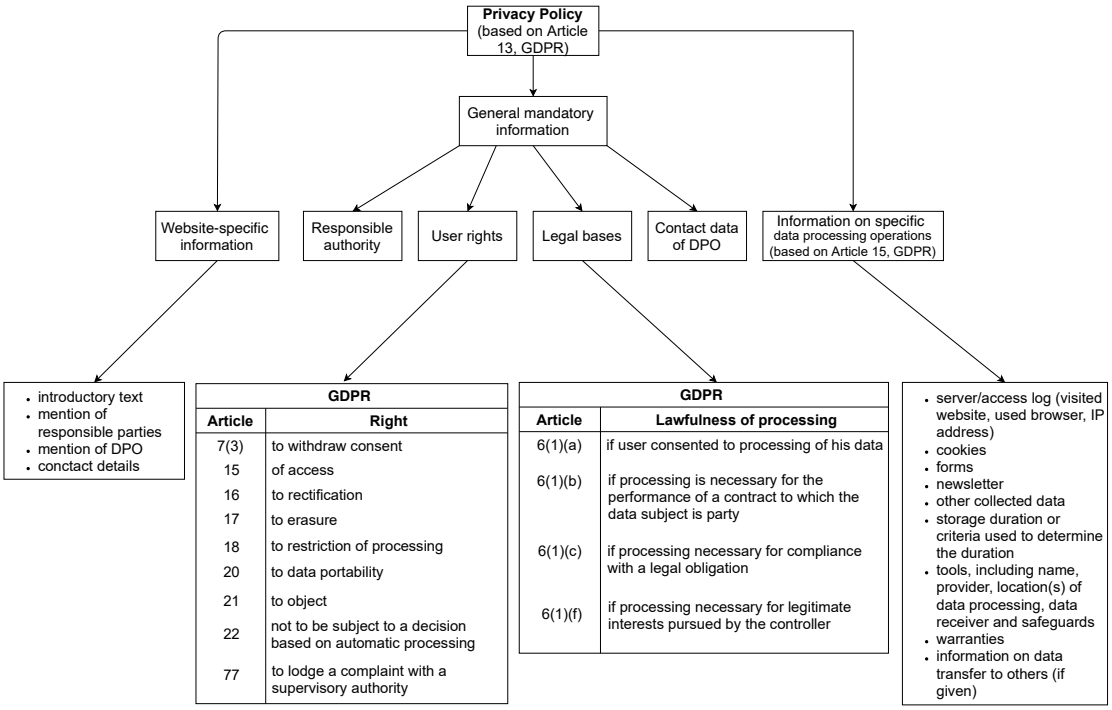


Figure 3.9: Contents of a privacy policy based on [9] and [62]

In the context of the privacy policy, the option to revoke (opt-out) must be offered at all times [22]. The legislator does not define how exactly privacy by default or design can be implemented, even though these principles are explicitly mentioned in Art. 25 [9]. It only cites pseudonymization as an example, and Recital 78 of the GDPR, which describes the TOM, also does not provide any further details regarding this. It is also possible to combine the consent with terms and conditions if it is visible that the declaration of consent is specific [34].

3.3.3 Cookies and storage periods

First-party cookies[4] are small packets of data that are generated by one's web browser and exchanged with a web server [63]. In return, only this server (as a first-party) has access to its cookie again later. A first-party cookie is defined as such that it can only be created and viewed by the operator of the website whose page one is visiting. Cookies that are generated by third-party sites (e.g., via advertisements) are called third-party cookies.

We categorize cookies into three types:

[4] Also known as "HTTP cookies".

- strictly necessary cookies
- functional cookies
- marketing cookies

Strictly necessary cookies allow us to navigate the website and to use its features, such as accessing protected areas of the website [63]. These cookies do not collect information about you that could be used for marketing purposes and do not remember the pages you have visited. Besides, they cannot be disabled, as this would limit the website's functionality. Functional cookies allow websites to remember our input (such as target audience, language, or the region we are in) and provide more personalized features. Without these cookies, a website cannot save a choice one has already made or customize the navigation experience. Marketing cookies collect information about browsing habits to do profiling on visitors. They record when a particular page has been visited and share this information with other parties, such as advertisers. When enabled, they can learn which services might be relevant to the visitor.

According to Art. 4(11) and Art. 7, consent is required before cookies can be set [9]. Under Recital 26 of the GDPR, cookies are considered personal data, implying that website owners have to use a cookie banner unless only strictly necessary cookies are being used.

3.3.4 Requirements for a deletion concept

Health data must be deleted when the purpose for collecting, processing, or storage has been fulfilled [9]. As stated in the section on legal bases, Art. 9(2) and 9(3) define exceptions for the deletion. According to Recital 39 of the GDPR, there are no uniform deadlines when personal data has to be deleted. Instead, each data controller's responsibility is to ensure that personal data is not stored for longer than necessary. This is achieved by establishing a deletion concept that regulates which data must be deleted under which conditions.

If users want their data to be deleted, they must be informed about the actions which were taken to delete their data or about reasons for why their request has been objected within one month [64]. In case of many requests, the platform operator can extend this deadline. If data is stored fore sole purpose retention obligations, the data can be made unavailable for access by most employees which would prevent that processed data is inconsistent with its specified purpose. It may pose a challenge to find out which data may be required and which data can be deleted. Therefore, the data controller should document that

the organization reviewed the issue and decided to keep storing the data until the duty to preserve records ends [65]. It is best practice to define when data needs to be deleted. As for scientific data, personal data may be retained on an extended basis for archival purposes [65].

It is suggested that the data controller regularly checks whether he is obliged to delete data, to which the guideline of the German Institute for Standardization (DIN) 66398 provides a suitable basis for [34]. Regarding the "right to be forgotten", companies also have to inform other data controllers if a user has requested the deletion of their data. The obligation to preserve records within the scope of medical treatment contracts is defined in several laws like Section 630(f) of the Civil Law Code [56].

The DIN standard 66398 describes how deletion rules can be controlled and implemented [66]. It suggests that one should differentiate between regulations for deletion and the execution of posed rules. Establishing those rules should be done by collaborating with different stakeholders, especially the DPO. After setting up those rules, it should be prioritized what needs to be deleted first. The idea is to differentiate between data types to create a framework where new data types can be integrated later on.

3.3.5 Breaches and responsible authorities

Data protection incidents are violations of the GDPR that are rendered less likely through proper compliance but can never be ruled out 100 percent. Particularly in the healthcare sector, with its sensitive data, there is a considerable risk that the responsible parties will suffer damage to their image and also be exposed to severe fines.

If data has been corrupted intentionally or if someone was given data unintentionally, it is considered a breach under Art. 4(12)[9]. In this context, it is also essential to check whether the incident constitutes a breach or whether, for instance, there was no risk to the rights of the data subject. Suppose the examination has shown that the incident in question is to be classified as a data protection incident. In that case, the responsible party has a maximum of 72 hours (including weekends, and holidays) to act from the time of becoming aware of the incident.

The Data Protection Conference, which is an independent data protection authority in Germany, has published guidance on assessing risk in its short paper no. 18 [67]. If the risk assessment reveals that there is likely to be a high risk to

the personal rights of data subjects, the users whose data were the subject of the emergency must also be notified in accordance with Art. 34 of the GDPR.

However, handling a data breach does not end with notifying the supervisory authority. When informing the authority, the company already has to provide the information as to what measures have been taken to minimize the risk. Therefore, part of documenting the incident is also the implementation of appropriate measures to prevent another data protection incident of this type. Even if the risk assessment does not result in a report of the incident to the competent supervisory authority, the incident identified must nevertheless be documented accordingly per Art. 33(5) of the GDPR [9]. This serves to inform the supervisory authority in the event of an audit, which is the basis for this decision. A key point is also the prompt involvement of the DPO during data mishaps. The majority of data breaches are caused by internal hacks [68]. To avoid data breaches, it is indispensable to train staff as improper training may lead to higher sanctions.

3.4 Summary

This chapter included key points of several GDPR-related articles. Not only did we outline user rights, we also emphasized the responsibilities that companies need to take care of. A DPMS can help with complying with the GDPR, and it is beneficial to use ISO standards to put procedures into place. Since the GDPR overlaps with other regulations, we have mapped similar articles or articles that give supplementary information. Especially in Germany, the FDPA should be taken into consideration when aiming for GDPR-compliance. To ensure that appropriate measures are implemented, and all processing operations are properly documented per Art. 30 GDPR, we have concluded best-practices like the contents of a privacy policy or storage periods.

4

Application of elaborated findings on eHealth platforms

In this chapter, we will first put together our earlier findings concisely to facilitate the compliance process for platform operators in the area of eHealth. Then, we will apply the results to eSano, where we will evaluate essential requirements of a GDPR-compliant eHealth application.

4.1 Impact of the GDPR on the eHealth sector

Without a doubt, we can argue that the GDPR has a considerable impact on the eHealth sector. As a general rule, any use of health data is subject to data privacy which makes Art. 9 of the GDPR the most significant one, as it has to be considered during every process. Therefore, health data processors must review their business practices in light of these legal justifications and adjust them to comply with these justifications.

Since laws at the federal level affect how data in each EEA country needs to be handled, we can look at the GDPR as the “tip of the iceberg” of legislation. For instance, patients need to give explicit consent per Art. 9(2) of the GDPR during genetic screenings [9], while genetic-related legislation in Germany further requires written permission by the responsible physician [34]. Other federal laws in Germany can be seen in Figure 2.5.

4.1.1 Decision tree to comply with legislation

To facilitate the process for organizations to determine whether they comply with significant articles of the GDPR, we have summed up the decisions organizations need to take in Figure 4.1.

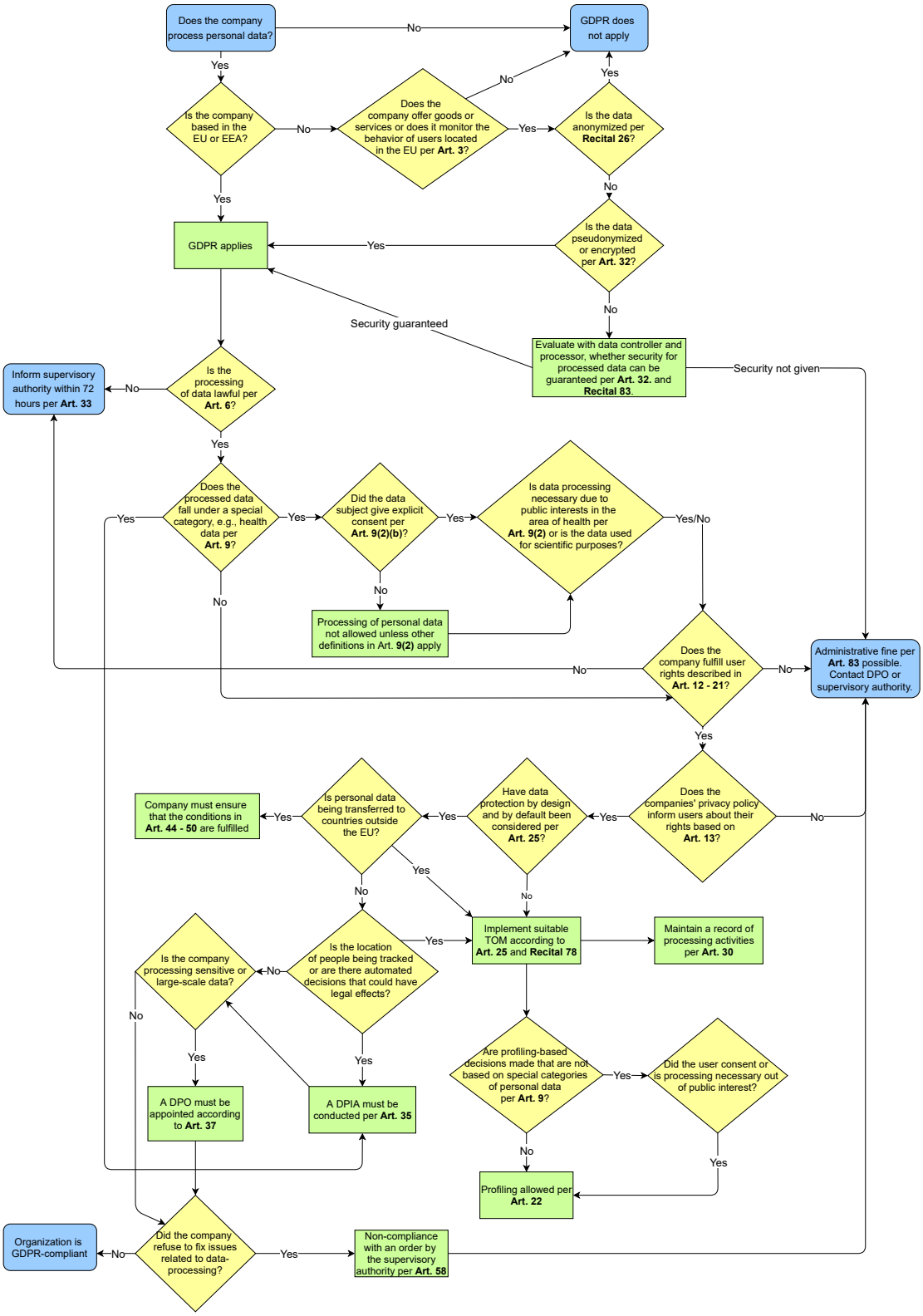


Figure 4.1: Decision tree to comply with the most relevant aspects of the GDPR based on [9]

The flowchart represents a decision tree. Each symbol, i.e., an oval, rectangle, or rhombus, indicates a start/end, a process, or a decision, respectively. The decision tree starts by examining the territorial scope of the company and whether the data is anonymized or pseudonymized. After that, we discuss which category the processed data falls upon. Once this has been clarified, we validate whether user rights' are fulfilled or not. Data protection by design, TOM and a DPIA have to be considered depending on each case. If a company does not comply with the GDPR even though it has to, it will be subject to fines according to Art. 83 of the GDPR [9].

4.1.2 Lawful processing of patient data

If data of a patient or user has been processed, and the user wants to know which data that is, Art. 14 of the GDPR allows data controllers to decline the provision of information under certain circumstances [9]. This could be the case if the user already has the data. Beyond this, there are no further information obligations if, for example, the provision of information proves to be impossible or requires a disproportionate effort, if the data is subject to confidentiality or if the data collection is specifically regulated by law.

As stated in Section 2.1.3, the GDPR gives reasons for personal data to be deleted in Art. 17, for instance, in case of no retention obligations that oppose deletion [9]. Section 630(f)(3) of the GCC imposes an obligation to retain patient files for at least ten years after completion of treatment [56].

Art. 25 of the GDPR already postulates that the basic principle of Art. 5 of the GDPR must be considered during the planning phase [9]. Even though Art. 25 GDPR only addresses the responsible people and not the data processors, Art. 28(1) GDPR allows collaboration with data processors only if they have implemented "privacy by design" and "privacy by default" to a sufficient degree [55].

Recital 159 of the GDPR elaborates on processing personal data for scientific research purposes [9]. It defines that "[...] scientific research purposes should be interpreted broadly, including technological development and demonstration, fundamental research, applied research, and privately funded research." [9, Recital 159].

4.1.3 Health-app providers' responsibilities in Germany

eHealth providers in particular must satisfy many requirements, and we will discuss this specifically in Chapter 5.2. We have summed up important regulations in Figure 4.2.

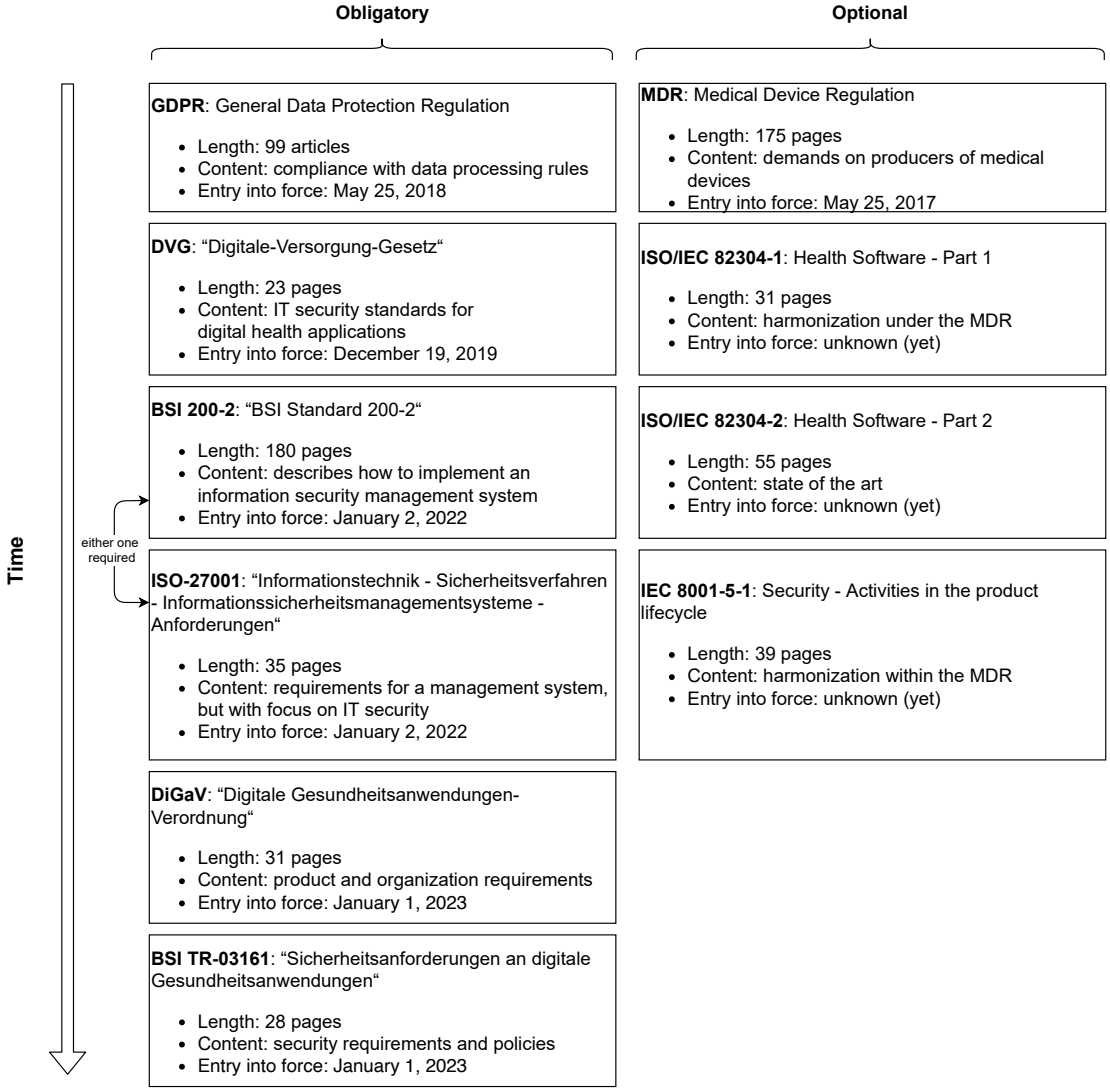


Figure 4.2: "Data security" requirements for eHealth applications based on [69]

The overview in Figure 4.2 depicts regulations that impose data security demands. We differentiate between obligatory and optional requirements. The timeline on the left shows which regulations and norms have already been enforced and the

ones that will be enforced in the future. Although the British Standards Institution (BSI) 200-2 and ISO-27001 will be implemented on January 2, 2022, only the realization of either one is necessary [69]. The Johner Institute argues that a process model can help to comply with the regulations and to mitigate efforts when designing other processes [69]. Security costs time and money which makes it a difficulty as a lack of security could cost money and negatively impact the image of a company on top of that.

4.1.4 Checklist for eHealth-platform operators

We have created three checklists consisting of a total of 20 questions that cover the most important articles and recitals of the GDPR. They also include articles of the FDPA, which can be ignored if the company is not based in Germany. Figure 4.3 covers the first ten questions.

No.	Legal basis	Title	Legal obligation	Yes	No	In parts	Not relevant
1	• Art. **30** GDPR	• Records of processing activitities	Do the data controller and data processor maintain a record of processing activities?	☐	☐	☐	☐
2	• Art. **9(1)** GDPR	• Processing of special categories of personal data	Does the company process personal data?	☐	☐	☐	☐
3	• Art. **9(2)** GDPR	• Processing of special categories of personal data	Does the company process sensitive personal data?	☐	☐	☐	☐
4	• Art. **37** GDPR • Art. **39(1)(e)** GDPR • Section **38(1)** FDPA	• Designation of the data protection officer • Tasks of the data protection officer • Data protection officers of private bodies	Has a data protection officer been appointed?	☐	☐	☐	☐
5	• Art. **38** GDPR • Recital **97** • Section **6** FDPA	• Position of the data protection officer • Data Protection Officer • Position	Is the company informed about the rights of a data protection officer?	☐	☐	☐	☐
6	• Art. **28** GDPR • Art. **29** GDPR • Art. **32** GDPR	• Processor • Processing under the authority of the controller and processor • Security of processing	Has the task of data processing been transferred to a processor?	☐	☐	☐	☐
7	• Art. **35** GDPR • Recital **75**	• Data protection impact assessment • Risks to the Rights and Freedoms of Natural Persons	Is there a high risk to the rights and freedoms of users?	☐	☐	☐	☐
8	• Art. **35** GDPR • Art. **36(1)-(3)** GDPR • Recital **75** • Recital **90**	• Data protection impact assessment • Prior consultation • Risks to the Rights and Freedoms of Natural Persons	If No. 7 was answered with 'Yes', has a Data Protection Impact Assessment been carried out?	☐	☐	☐	☐
9	• Art. **4(12)** GDPR • Art. **33** GDPR • Art. **58(1)** GDPR • Recital **85** • Recital **87** • Section **42(4)** FDPA • Section **43(4)** FDPA	• Personal data breach • Notification of a personal data breach to the supervisory authority • Powers • Notification Obligation of Breaches to the Supervisory Authority • Promptness of Reporting/Notification • Penal Provisions • Provisions on administrative fines	In case of a personal data breach, does the company have right procedures in place to report, identify and investigate the breach?	☐	☐	☐	☐
10	• Art. **32** GDPR • Recital **83**	• Security of processing	Did the organization take appropriate Technical and Organizational Measures to ensure that data processing is secure?	☐	☐	☐	☐

Figure 4.3: Obligations of the data processor based on [70], [9] and [47]

The checklist in Figure 4.3 consists of questions related to the responsibilities of the data processor. The column “Legal basis” is sorted ascendingly and starts with articles and recitals of the GDPR and rounds it off with sections from the FDPA. The column “Legal obligation” contains the corresponding title of the respective article stated on the legal basis. The legal obligation to appoint a DPO when working with health-related data is inevitable as health data is categorized as sensitive data [9].

No.	Legal basis	Title	Legal obligation	Yes	No	In parts	Not relevant
11	• Art. **6(1)(f)** GDPR • Art. **13** GDPR • Art. **22(1), 22(4)** GDPR • Art. **27** GDPR • Art. **44** GDPR • Art. **77** GDPR	• Lawfulness of processing • Information to be provided where personal data are collected from the data subject • Automated individual decision-making, including profiling • Representatives of controllers or processors not established in the Union • General principle for transfers • Right to lodge a complaint with a supervisory authority	Does the company know what information obligations they have, if (only) they process the collected user data?	☐	☐	☐	☐
12	• Art. **6(1)(f)** GDPR • Art. **13-22** GDPR • Art. **26(2)** GDPR • Art. **27** GDPR • Art. **44** GDPR • Art. **77** GDPR • Art. **89(1)** GDPR • Recital **60** • Recital **61** • Recital **62** • Section **29(1)** FDPA • Section **33** FDPA	• Lawfulness of processing • Joint controllers • Representatives of controllers [...] • General principle for transfers • Right to lodge a complaint [...] • Safeguards [...] • Information Obligation • Time of information • Exceptions to the Obligation to Provide Information • [...] secrecy obligations • Information to be provided where personal data have not been obtained from the data subject	Does the company know what information obligations they have, if user data has been processed by other organizations?	☐	☐	☐	☐
13	• Art. **5(2)** GDPR • Art. **12** GDPR • Art. **15** GDPR • Recital **63** • Recital **64** • Section **34(1)-(2)** FDPA	• Purpose limitation • Transparent information [...] • Right of access by the data subject • Right of access • Identity verification • Right of access by the data subject	Can the data controller provide information about the data it stores from users and are they capable of providing a copy of the data upon request?	☐	☐	☐	☐
14	• Art. **5(2)** GDPR • Art. **12(1), 12(3), 12(6)** • Art. **16** GDPR • Art. **19** GDPR	• Purpose limitation • Transparent information [...] • Right to rectification • Notification obligation [...]	Can the data controller correct inaccurate data?	☐	☐	☐	☐
15	• Art. **4(2)(e)** GDPR • Art. **5(1)(e)** GDPR • Art. **12** GDPR • Art. **17** GDPR • Art. **19** GDPR • Recital **26** • Recital **39** • Recital **65** • Recital **66** • Section **35** FDPA	• Definitions • Lawfulness, Fairness and transparency • Transparent information [...] • Right to erasure • [...] erasure of personal data [...] • Not Applicable to Anonymous Data • Principles of Data Processing • Right to Rectification and Erasure • Right to be Forgotten	Can the data controller delete data if relevant prerequisites are satisfied?	☐	☐	☐	☐
16	• Art. **12** GDPR • Art. **20** GDPR • Recital **68**	• Transparent information • Right to data portability • Right of Data Portability	Upon request, can the data controller provide data of a user in a machine-readable format which can then be used by another controller?	☐	☐	☐	☐
17	• Art. **12** GDPR • Art. **21** GDPR • Recital **70**	• Transparent information • Right to object • Right to Object to Direct Marketing	Does the company know what to do if data subjects objects to processing their data or profiling?	☐	☐	☐	☐

Figure 4.4: Information obligations and data subject rights based on [70], [9] and [47]

The checklist in Figure 4.4 consists of questions related to information liabilities. It primarily refers to topics listed in Chapter 3 of the GDPR, i.e., user rights [9]. In this case, numerous recitals offer helpful explanations on what exactly is meant with each right.

No.	Legal basis	Title	Legal obligation	Yes	No	In parts	Not relevant
18	• Art. **6(1)** GDPR • Art. **13** GDPR • Art. **14** GDPR • Art. **21(1)-(4)** • Art. **35(7)(a)** GDPR • Recital **47**	• Lawfulness of processing • Information to be provided where personal data are collected from the data subject • Information to be provided where personal data have not been obtained from the data subject • Right to object • Data protection impact assessment • Legitimate Interest	Does a legal basis exist for the processing of user data?	☐	☐	☐	☐
19	• Art. **6(1)** GDPR • Art. **7** GDPR • Art. **8** GDPR • Art. **9** GDPR • Recital **32** • Recital **42** • Recital **43** • Recital **171**	• Lawfulness of processing • Conditions for consent • Conditions applicable to child's consent in relation to information society serves • Processing of special categories of personal data • Conditions for Consent • Burden of Proof and Requirements for Consent • Freely Given Consent • Repeal of Directive 95/46/EC and Transitional Provisions	Can the institution ensure and prove that a data subject has given appropriate consent for data collection and processing?	☐	☐	☐	☐
20	• Art. **6(1)** GDPR • Art. **7** GDPR • Art. **13** GDPR • Art. **14** GDPR • Recital **32** • Recital **50** • Section **24** FDPA	• Lawfulness of processing • Conditions for consent • Information to be provided where personal data are collected from the data subject • Information to be provided where personal data have not been obtained from the data subject • Conditions for Consent • Further Processing of Personal Data • Processing for other purposes by private bodies	Does the company meet specific conditions if data is being processed for a reason other than the one for which they were collected?	☐	☐	☐	☐

Figure 4.5: Legal bases for processing based on [70], [9] and [47]

The last checklist in Figure 4.5 clarifies the issue of a legal basis. Especially the aspect of consent is momentous as all aspects of data processing are based on appropriate user consent. Depending on the study that is conducted using eSano, users will be asked for their consent on paper. Currently, the eHealth platform will be used for online sessions for a study called “PSYCHOnlineTherapie”.

The declaration of consent can be seen in Appendix B. Some crucial contents of it are:

- involved parties, data flows and storage locations
- data collection and evaluation in a pseudonymized form
- deletion of contact data after the last participant has completed the last survey and data will only be available in anonymized form afterwards
- contact data of DPO
- user rights according to Art. 13(2) GDPR

We acknowledge that the consent form in Appendix B is very much in line with the legal obligations of the General Data Protection Regulation.

4.2 GDPR with regard to the eHealth platform eSano

Now that we have analyzed the impact of the GDPR on eHealth developers in Section 4.1, we continue with assessing the current state of eSano in the context of the GDPR. We will do that by comparing the current implementation of certain aspects with how they could look in the best-cases. We will cover Chapter 4 by applying the flow chart in Figure 4.1, as well as the checklists on eSano.

4.2.1 Applying the decision tree on eSano

We start by applying the decision tree in Section 4.1.1 on eSano. First and foremost, the institute does process personal data with eSano. The platform is based in Germany as it was developed and designed by the University of Ulm. It also offers services per Art. 3 GDPR, which means that the GDPR applies. According to Art. 32 GDPR [9], the collected data is stored in encrypted form on the servers of STRATO AG in Germany (see Appendix C). Per Art. 6 of the GDPR eSano allows users to consent to processing their data [9]. In fact, the processed data falls under a special category, i.e., health data under Art. 9(2)(h) and Recital 35. Therefore, the next obligation is to comply with user rights stated in Art. 12 – 21 GDPR [9]. Most of these articles have been taken into account via the privacy policy in Appendix C which is required under Art. 13 GDPR. We will analyze this in detail in Section 4.2.2. Especially the right to erasure (Art. 17 GDPR) has been taken care of by implementing a function which allows users to request the deletion of their account.

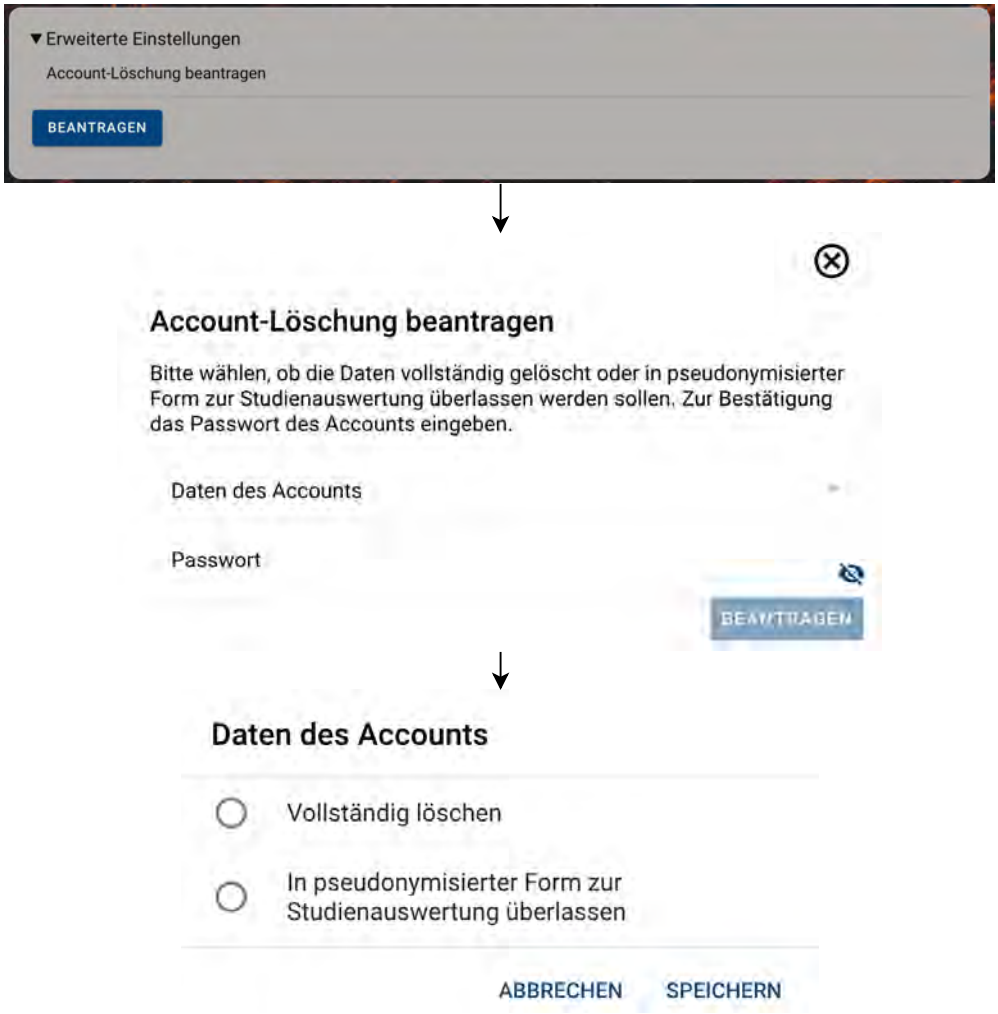


Figure 4.6: eSano (patient) account deletion process from [71]

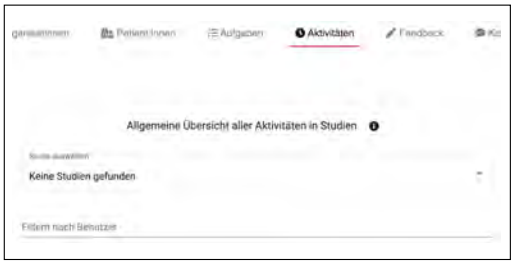
Figure 4.6 shows that users can click on the blue button to request the deletion of their account. Once clicked, they will then be asked whether their data should be deleted completely or if the data can be used in pseudonymized form for analyzing studies.

Data Protection by design and by default have also been considered per Art. 25 GDPR [9]. This can be proven by looking at the documentation and the implemented functions. The Software Requirements Specification included (functional) requirements relevant for this aspect. We have summarized some of them in Figure 4.7.

ID	FA-T01
DES	Confidentiality of patient information
MOT	By default, eCoaches are only allowed to see the activities of their own patients. Exceptions are representations or emergencies. The eCoaches have the possibility to see when their own patients were last online. In addition, eCoaches can see all patients who are in a group/study with them, but not their exact activities.
DEP	
SUBP	eCoach platform
PRIO	++

ID	FA-F19
DES	Contact IT support
MOT	For all users of the system there should be the possibility to contact the IT support. This can be done via the help function of the system.
DEP	
SUBP	eCoach platform, patient application, cms
PRIO	0

ID	FA-G08
DES	Activity log of a group
MOT	The eCoach platform provides an activity log that displays any activities that are performed by their patients or any member of the study or the interventions in it. This log can only be seen by eCoaches and not by patients. The workgroups and organisationgroups have also activity logs.
DEP	
SUBP	eCoach platform, patient application, cms
PRIO	+



ID	FA-L03
DES	Reset password
MOT	All users of the system have the possibility to reset their password if they forget it. If their login fails, they can reset their password using their email address to create a new password.
DEP	
SUBP	eCoach platform, patient application, cms
PRIO	++

Figure 4.7: Excerpt of functional requirements from the eSano platform and its internal Software Requirements Specification

No personal data is being transferred to countries outside the EU. However, a DPIA is required under Art. 35 GDPR since health-data is being processed [9]. Evidently, a DPO also had to be appointed according to Art. 37. The DPO is represented by the University of Ulm and can be contacted via e-mail [71]. The decision tree in Figure 4.8 points out the nodes we have traversed.

We have marked the path(s) we underwent in green in Figure 4.8. Even before starting this thesis we knew that the GDPR does apply on eSano because otherwise we would not have been able to apply the research conducted in Chapter 2. Therefrom, our primary focus is the adherence of eSano with articles focusing on protecting user data. We can consider this decision tree like an initial screening that already filters out some important aspects. For instance, we now know that eSano does not transfer personal data to countries outside the EU and that we do have a legal basis processing user data.

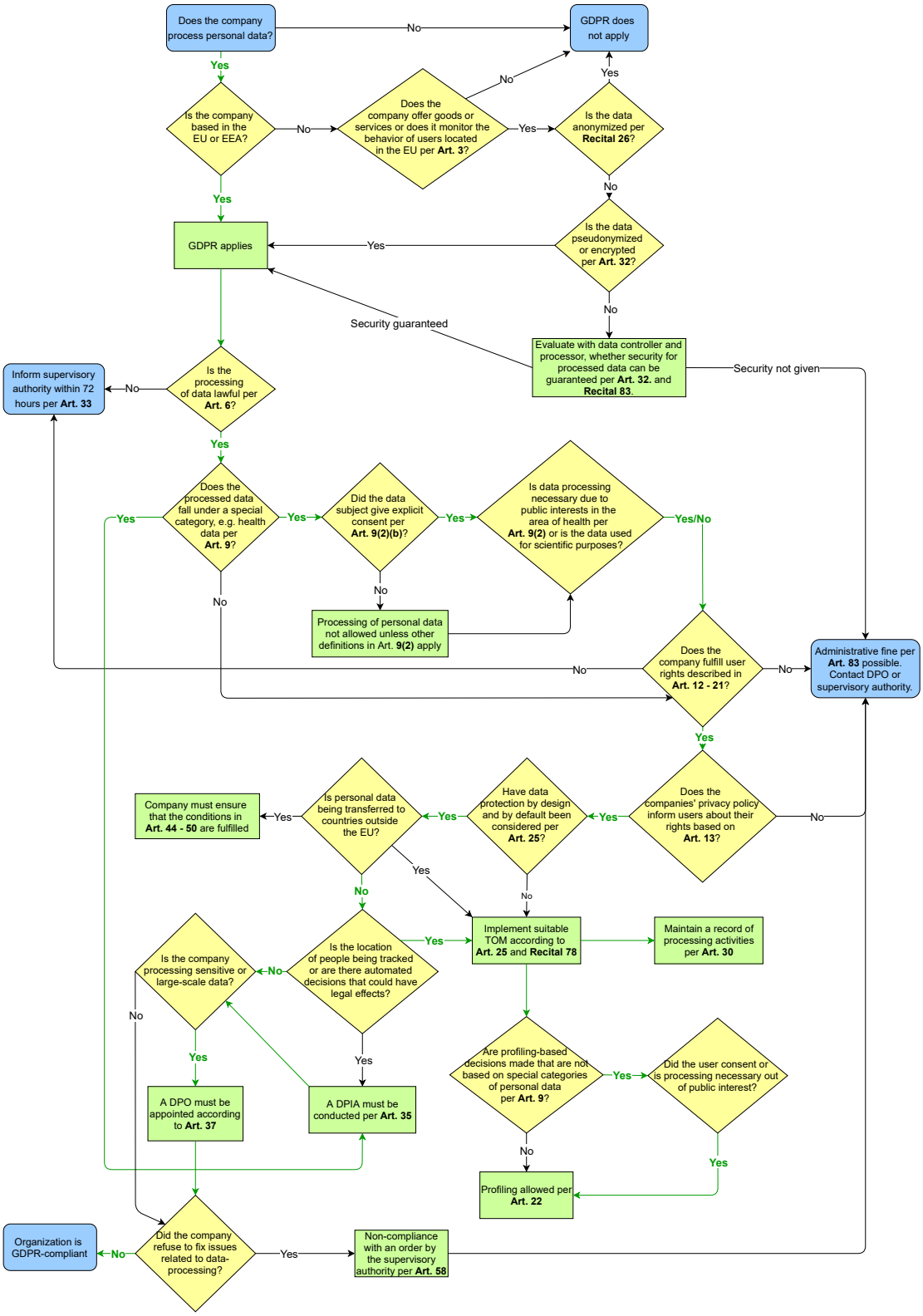


Figure 4.8: Applied decision tree based on [70], [9] and [47]

4.2.2 Privacy Policy AS/IS versus TO/BE

AS/IS	TO/BE + OPTIONAL
Dear users of the eSano platform, the protection of your personal data is important to us. Therefore, we inform you here about the purpose for which we collect, store or forward your data. If you use this platform as part of a study, further data protection requirements may apply in the associated participation information or consent forms. This information also tells you what rights you have with regarding your personal data.	**Dear users of the eSano platform,** the protection of your personal data is important to us. When using our platform as part of a study, further data protection requirements may apply in the associated participation information or consent forms. We process personal data only to the extent necessary to provide functions or services, if possible. The processing of personal data such as name, address, e-mail address or telephone number is always in accordance with the General Data Protection Regulation (GDPR)* and the BDSG. In the following, we provide information about the type, scope and purpose of the personal data we collect, use and process. Furthermore, we inform data subjects of the rights to which they are entitled to through this privacy policy. Questions, comments and requests regarding our privacy policy can be sent to us at any time using the contact form. You can reach our data protection officer at dsb@uni-ulm.de.
1. Responsible person for data processing The person responsible for data processing is named according to Art. 4(7) of the General Data Protection Regulation (GDPR) as follows University of Ulm 89069 Ulm Telephone +49 (0)731/50-10 Fax +49 (0)731/50-22038 The University of Ulm is a public corporation which is represented by president Prof. Dr.-Ing. Michael Weber praesident@uni-ulm.de or by chancellor Dieter Kaufmann kanzler@uni-ulm.de. If you have any questions regarding data protection, please contact dsb@uni-ulm.de or send a letter with the addition "Data Protection Officer" to the address given above. For more specific information regarding the particular study you are participating in, please refer to the associated participation information or declaration of consent.	**1. Person responsible for data processing** The person responsible for data processing is named according to Art. 4(7) of the GDPR: Address: University of Ulm 89069 Ulm Telephone: +49 (0)731/50-10 Fax: +49 (0)731/50-22038 E-mail address: dsb@uni-ulm.de* The University of Ulm is a public body represented by president Prof. Dr.-Ing. Michael Weber praesident@uni-ulm.de or by Chancellor Dieter Kaufmann kanzler@uni-ulm.de. If you have any questions regarding data protection, please contact dsb@uni-ulm.de or send a letter with the addition "Data Protection Officer" to the address above. For more specific information regarding the particular study you are participating in, please refer to the related participation information or declaration of consent.

Figure 4.9: “eSano” Privacy Policy Part I based on Appendix C, [71] and [9]

AS/IS	TO/BE + OPTIONAL
2. Data categories, purpose and legal basis of data processing [...] All data collected via the platform is stored in encrypted form on STRATO AG servers located in Germany. The following personal data will be processed from you: - E-mail address - Entries in interventions and diaries - Conversations with e-coaches and other users - Usage data of the platform with regard to general usage behavior (e.g., time of logins) as well as the online intervention program (e.g., start time point of processing, completion time of a lesson) [...] The legal basis for the processing is your consent to participate in the respective study according to Art. 6(1)(a) GDPR. If vital interests of the data subject or another natural person requires processing of personal data, Art. 6(1)(d) GDPR serves as the legal basis. Furthermore, health data are processed according to Art. 9(1) GDPR, which are collected as part of a study. Health data includes all data that provide information about the physical or mental condition and relate to a natural person. Health data is only processed with your explicit consent in accordance with Art. 9(2)(a) GDPR. Only through this consent, it is possible to use the eSano platform without restrictions. [...] Cookies that are necessary for the exercise of electronic communication processes or the provision of certain functions desired by you (e.g. shopping cart) are set based on Art. 6(1)(f) GDPR. [...] In server log files, we automatically collect and store information that your browser automatically transmits to us and that is necessary to ensure the proper functionality of the platform as well as its stability and security (the legal basis for this is Art. 6(1)(f) GDPR): - Visited site on our domain - Browser type and version - Operating system referrer URL - Host name of the accessing computer - Date and time of server request - IP address	**2. Data categories, purpose and legal basis of data processing** [...] All data collected via the platform is stored in encrypted form on STRATO AG servers located in Germany. The following personal data will be processed from you: - E-mail address - Entries in interventions and diaries - Conversations with e-coaches and other users - Usage data of the platform regarding general usage behavior (e.g., time of logins) as well as the online intervention program (e.g., start time point of processing, completion time of a lesson) [...] The legal basis for the processing is your consent to participate in the respective study according to Art. 6(1)(a) GDPR. Art. 6(1)(b) GDPR serves as the legal basis when processing personal data that is needed for the fulfillment of a contract for which the data subject is a contractual party. The same applies to processing operations that are required for the implementation of pre-contractual measures.* If processing of personal data is necessary for compliance with a legal obligation to which our platform is subject, Art. 6(1)(c) GDPR serves as the legal basis.* If vital interests of the data subject or another natural person requires processing of personal data, Art. 6(1)(d) GDPR serves as the legal basis. Furthermore, health data are processed according to Art. 9(1) GDPR, which are collected as part of a study. Health data includes all data that provide information about the physical or mental condition and relate to a natural person. Health data is only processed with your explicit consent in accordance with Art. 9(2)(a) GDPR. Only through this consent, it is possible to use the eSano platform without restrictions. In the context of processing personal data for further scientific and regulatory purposes, we do not use fully automated decision-making under Article 22 GDPR. [...] Cookies that are necessary for the exercise of electronic communication processes or the provision of certain functions desired by you (e.g. shopping cart) are set based on Art. 6(1)(f) GDPR. [...] Our website collects a series of general data and information with each call of a page by you or an automated system to ensure the proper functionality of the platform as well as its stability and security. The legal basis for this is Art. 6(1)(f) GDPR. The collected data and information stored in the log files of the server can be: - Visited site on our domain - Browser type and version - Operating system referrer URL - Host name of the accessing computer - Method (e.g. GET, POST), date and time of the server request - Date and time of server request - IP address of the requesting device Please note that in order to fulfill your contact request, we may also send you e-mails to the address provided. This has the purpose that you can receive a confirmation from us that your request has been correctly forwarded to us. However, the sending of this confirmation e-mail is not obligatory for us and is only for your information.
3. TLS encryption For security reasons and to protect the transmission of confidential content that you send to us as the site operator, our website uses SSL and TLS encryption. This means that the data you transmit via this platform cannot be read by third parties. You can recognize an encrypted connection by the "https://" address line of your browser and the lock symbol in the browser line.	**3. SSL/TLS encryption** For security reasons and to protect the transmission of confidential content that you send to us as the site operator, our website uses SSL and TLS encryption. This means that the data you transmit via this platform cannot be read by third parties. You can recognize an encrypted connection by the "https://" instead of a "http://" in the address line of the browser and by the lock symbol in your browser line.
4. Storage of your data Provided that no other legitimate interests of the controller oppose deletion, deletion will take place when you participate in a study or in a research project in accordance with the storage period specified there. If you use the platform in the context of a study, you will find further specific information in the associated participation information or the declaration of consent. In this regard, please inform yourself about the deletion period within the scope of the corresponding study or research project. Your data will be stored as long as it is needed for the proper functionality of the platform, at the latest, until your account is deleted. If your account is deleted, your personal data will be deleted or the personal reference removed.	**4. Storage of your data** The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. Provided that no other legitimate interests of the controller oppose deletion, deletion will take place when you participate in a study or in a research project in accordance with the storage period specified there. If you use the platform in the context of a study, you will find further specific information in the associated participation information or the declaration of consent. In this regard, please inform yourself about the deletion period within the scope of the corresponding study or research project. Your data will be stored as long as it is needed for the proper functionality of the platform, at the latest, until your account is deleted. If your account is deleted, your personal data will be deleted or the personal reference removed.

Figure 4.10: “eSano” Privacy Policy Part II based on Appendix C, [71] and [9]

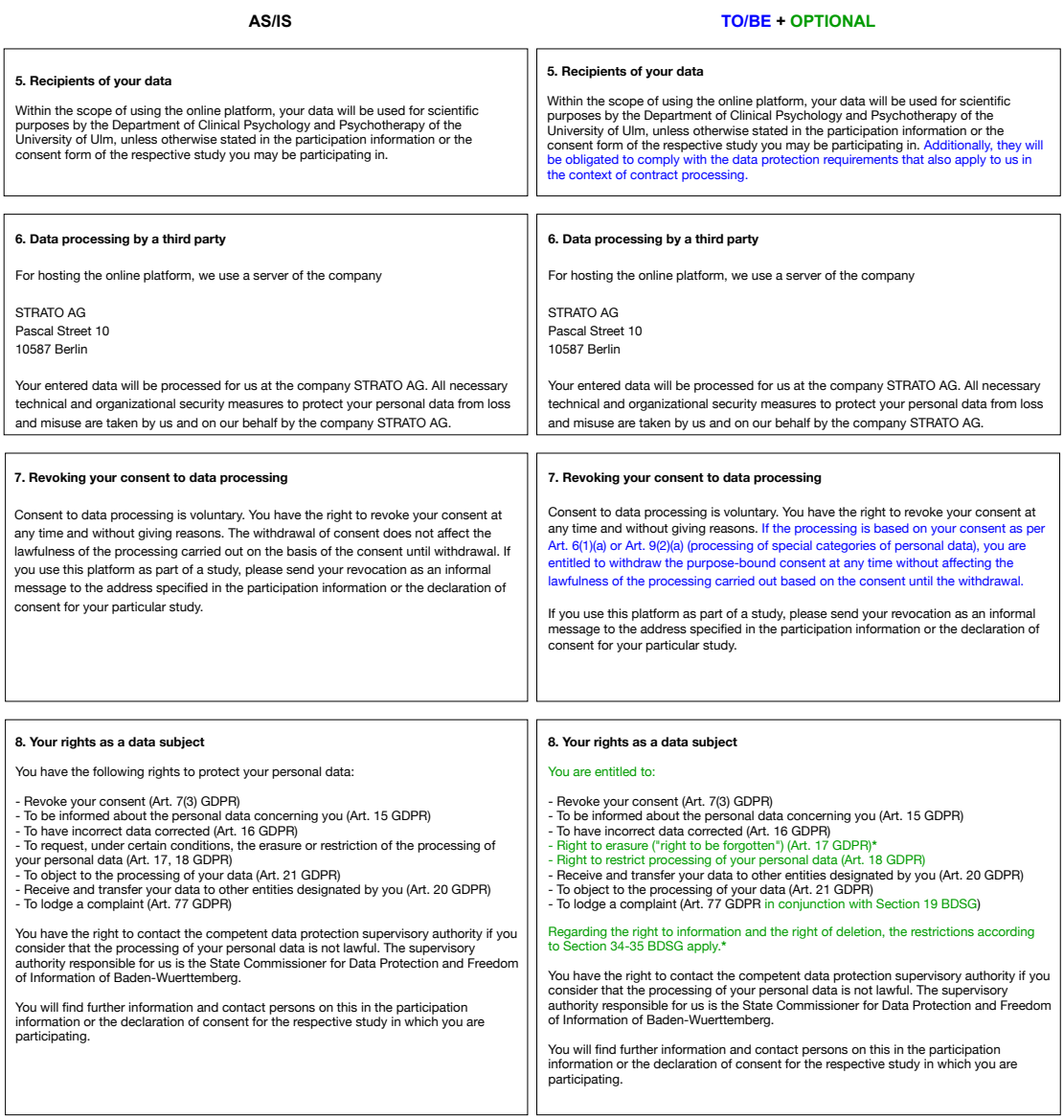


Figure 4.11: "eSano" Privacy Policy Part III based on Appendix C [71] and [9]

We have divided the privacy policy of eSano into three parts as we would not be able to fit it on one page. The privacy policy is written in German and can be seen in original in Appendix C. For consistency purposes we have translated it into English accordingly, which can be seen in the "AS/IS". The "TO/BE" (blue) and "OPTIONAL" (green) part reflect amendments we have put inside the privacy policy. We will explain the parts that we have marked with an asterisk in the images in more detail here. As for Figure 4.9, it may be beneficial to mention the GDPR in the introductory text. Referring to the GDPR in the first paragraph

already prepares users mentally for what comes next. Keeping context-relevant details abstract without separating it into different parts, keeps the privacy policy user-friendly. For instance, it is easier to find the E-Mail of the DPO if it is right below the Fax instead of it being inside a paragraph as that may give the impression of covering something up.

Figure 4.10 emphasizes the importance of Art. 6(1)(b) and Art. 6(1)(c). Art. 6(1)(b) is relevant insofar as data processing is lawful if it is necessary for the performance of a contract or pre-contractual measures [9]. As users participate in studies (using eSano as platform), storing user inputs becomes a prerequisite. For Art. 6(1)(c), eSano and other entities using the platform are subject to various legal obligations. This info might not be trivial for data subjects using eSano.

The privacy policy in Figure 4.11 can be polished with some additional information. Especially the notes we marked with the asterisk, i.e., the right to erasure must be stated. Here, we explicitly refer to Section 3.3.4 again, where we elaborated the circumstances for data deletion and retention periods. Since Germany complemented the GDPR with other federal laws, some articles are in conjunction with other ones. For instance, the privacy policy can state that Art. 77 GDPR is in conjunction with Section 19 of the FDPA. For this aspect, we refer to the interfaces between GDPR and FDPA in Section 3.2.2. Overall, we note that the privacy policy of eSano is matching with the contents we outlined in Section 3.3.2.

4.2.3 DPIA AS/IS versus TO/BE

Substantial parts of the DPIA described in Figure 3.4 have been conducted for eSano. We can see this by looking at specific parts of the documentation for eSano. For instance, per Appendix D, new project members are briefed on the relevance of data protection. Permissions for different systems like Gitlab[1] and Mattermost[2] are given based on least privilege, meaning that members only receive access rights for their specific tasks. Users are also introduced to “secure coding” standards per Appendix E. However, it is not clear whether project members have to familiarize themselves with those standards alone or with the help of a peer. In the context of a DPIA, it may be better to create a separate document which enlists the responsibilities of each member and defines who verifies their realization.

[1] Platform for project- and source code management.
[2] Platform for communication and collaboration.

The responsible people for the eSano platform have multiple documents for a risk evaluation. For instance, the documentation regarding risk management for eSano categorizes three parts: data integrity, product functionality and patient safety. They also evaluate each risk by judging its severity and frequency. Therefore, a risk assessment based on part three of the DPIA in Figure 3.4 has been carried out for eSano. The risk assessment can be seen in German in Appendix F. We have translated parts of it into English, and showcased the AS/IS and TO/BE comparison in Figure 4.12, 4.13 and 4.14.

AS/IS (Product functionality)

Risk:	Usage becomes unattractive and patient dissatisfied
Cause:	No new lessons unlocked from eCoach
Prevention/Reduction:	Possibility to send messages to eCoach or "unlock new lesson" as a task/reminder
Comments:	
Severity	Critical (2) -> Critical (2)
Frequency	Occasionally (3) -> Rare (2)

TO/BE + OPTIONAL

Risk	Usage becomes unattractive and patient dissatisfied.
Description of the scenario	The platform becomes unattractive if eCoaches do not release or unlock new lessons frequently.
Affected Persons	User + eCoaches
Personal Data	None.
Involved Actors (involved parties)	User/Content Editor/eCoach
Possible damage for the affected person	Users become discontent and may even stop using the application. Potential study data is lost and eCoaches lose participants.
Trigger elements for the occurrence of damage	- Forgetting to unlock lessons. - Lack of variety.
Existing TOM	Variety of lessons established before starting a study.
Affected warranties	Rewarding users for study participation.
Severity of damage	Critical (2) -> Critical (2)
Probability of occurrence	Occasionally (3) -> Rare (2)
Corrective actions	Possibility to send messages to eCoach or "unlock new lesson" as a task/reminder.

Risk:	Data protection issue
Cause:	Saving the password on non-personal computer
Prevention/Reduction:	Warning message before saving the password (or in the text when logging in)
Comments:	
Severity	Critical (2) -> Critical (2)
Frequency	Rare (2) -> Theoretically possible (1)

Risk	Data protection issue
Description of the scenario	Users save their password(s) on devices which are not their own.
Affected Persons	Primarily users
Personal Data	User password
Involved Actors (involved parties)	Users/Content Editor/eCoach/Admins & Devs
Possible damage for the affected person	Password of the user could be stolen or misused.
Trigger elements for the occurrence of damage	- Using a device (laptop/computer/phone) which does not belong to the user. - Using insecure networks or public WiFi.
Existing TOM	Users can change their password by clicking the "Forgot password" button on the homepage.
Affected warranties	Preventing unauthorized access
Severity of damage	Critical (2) -> Critical (2)
Probability of occurrence	Rare (2) -> Theoretically possible (1)
Corrective actions	Warning message before saving the password (or in the text when logging in). Implementing a two-factor authentification.

Figure 4.12: Data Integrity risk assessment based on Appendix F and [44]

AS/IS (individual-related)

Risk:	Usage becomes unattractive and patient dissatisfied
Cause:	No new lessons unlocked from eCoach
Prevention/Reduction:	Possibility to send messages to eCoach or "unlock new lesson" as a task/reminder
Comments:	
Severity	Critical (2) -> Critical (2)
Frequency	Occasionally (3) -> Rare (2)

TO/BE + OPTIONAL

Risk	Usage becomes unattractive and patient dissatisfied.
Description of the scenario	The platform becomes unattractive if eCoaches do not release or unlock new lessons frequently.
Affected Persons	User + eCoaches
Personal Data	Study-dependent.
Involved Actors (involved parties)	User/Content Editor/eCoach
Possible damage for the affected person	Users become discontent and may even stop using the application. Potential study data is lost and eCoaches lose participants.
Trigger elements for the occurrence of damage	- Forgetting to unlock lessons - Lack of variety
Existing TOM	Variety of lessons established before starting a study.
Affected warranties	Rewarding users for study participation.
Severity of damage	Critical (2) -> Critical (2)
Probability of occurrence	Occasionally (3) -> Rare (2)
Corrective actions	Possibility to send messages to eCoach or “unlock new lesson” as a task/reminder.

Risk:	Platform usage becomes unattractive, eCoach dissatisfied and/or useless workload
Cause:	Patient does not conduct intervention properly, becomes verbose, sends or answers inappropriate texts
Prevention/Reduction:	Reporting function (mediator: eCoach manager, who has access to patient's answers and message history). eCoach can delete patients or exclude them from the study
Comments:	Alternatively also study hotline/-mail, contact person
Severity	
Frequency	

Risk	Platform usage becomes unattractive, eCoach dissatisfied and/or useless workload
Description of the scenario	Patients do not perform interventions as intended. They become conspicuous and send inappropriate texts
Affected Persons	Users
Personal Data	Data related to the study they are participating in and chat messages.
Involved Actors (involved parties)	Users/Content Editor/eCoach
Possible damage for the affected person	Platform usage might affect users mental health negatively. Study data might become inaccurate.
Trigger elements for the occurrence of damage	- Intervention(s) incomplete - Lack of correspondence with eCoach
Existing TOM	- Chat function - Diary function
Affected warranties	- Rewarding users for participating in studies - Protection of user health per MDR
Severity of damage	Low (1) -> Low (1)
Probability of occurrence	Rare (2) -> Theoretically possible (1)
Corrective actions	Reporting function (mediator: eCoach manager, who has access to patient's answers and message history). eCoach can delete patients or exclude them from the study.

Figure 4.13: Product functionality risk assessment based on Appendix F and [44]

AS/IS (individual-related)

Risk:	Self-harming behavior, possibly suicide
Cause:	Suicidal thoughts/threats sent via message to eCoach which is not read or responded to
Prevention/Reduction:	Contact options can be limited (e.g., PSYCHOnlineTHERAPIE), specification of emergency help numbers (crisis hotline)
Comments:	
Severity	
Frequency	

TO/BE + OPTIONAL

Risk	Self-harming behavior, possibly suicide
Description of the scenario	A user starts to harm himself or commits suicide in the worst case.
Affected Persons	User
Personal Data	Messages to eCoach.
Involved Actors (involved parties)	User/eCoach/Admins/Devs
Possible damage for the affected person	User hurts himself, physically or mentally
Trigger elements for the occurrence of damage	- Lack of (personal) support - Unread messages - Lack of engagement - Failure to understand users
Existing TOM	Variety of lessons established before starting a study.
Affected warranties	- Ensuring the safety of the platform per MDR. - Fowarding personal data without consent
Severity of damage	Critical (2) -> Critical (2)
Probability of occurrence	Theoretically possible (1) -> Theoretically possible (1)
Corrective actions	Contact options can be limited (e.g., PSYCHOnlineTHERAPIE), specification of emergency help numbers (crisis hotline)

Risk:	No help through online lessons
Cause:	Online lessons are not being accessed or used by users
Prevention/Reduction:	Reminder for interventions that are still pending
Comments:	
Severity	
Frequency	

Risk	No help through online lessons
Description of the scenario	Online lessons are not being accessed or used by users.
Affected Persons	Users
Personal Data	Data related to the study they are participating in and chat messages.
Involved Actors (involved parties)	Users/Content Editor/eCoach
Possible damage for the affected person	Platform usage might affect users mental health negatively. Study data might become inaccurate.
Trigger elements for the occurrence of damage	- Platform unavailable. - Wrongly configured interventions - Lack of engagement from user(s) - Intervention(s) incomplete - Lack of correspondence with eCoach
Existing TOM	eCoaches can chat with users.
Affected warranties	Failure to complete study
Severity of damage	Low -> Low
Probability of occurrence	Theoretically possible (1) -> Rare (2)
Corrective actions	Reminder for interventions that are still pending. Regular meetings to improve interventions.

Figure 4.14: Individual-related risk assessment based on Appendix F and [44]

Currently, the risk assessment in Figure 4.12 considers five criteria, that is, risk, cause, prevention, severity, and frequency. However, it would be best-practice to consider various categories and subcategories (physical, tangible, intangible, etc.) [44]. In the "TO/BE" section we have included criteria that should be considered for each risk. While the current documentation considers what causes risk and how they can be prevented, it does not specify the kind of damage those risks could cause, which entities get affected, and which TOM already exist. We have elaborated on two risks: data loss and data protection. Regarding data loss, triggering factors could not only be an internet disconnection, but also causes like network or server issues. For instance, data may get lost if a server does not respond. Affected warranties could therefore not only be the loss or protection of personal data, but also a faulty performance by the data processor, i.e., STRATO AG. As for the risk "data protection issue", it may also be good to differentiate between the involved actors. Depending on the affected entity, e.g., a content editor or an eCoach, corrective actions may differ.

The risks regarding product functionality in Figure 4.13 are described vaguely and have potential for a detailed portrayal. The risk of the occasional user being dissatisfied with an intervention is possible, but it is even more important that eCoaches and Content Editors do not become satisfied as this may impact how patients are supported when using the platform. Numerous features have already been implemented to tackle these problems, but the aspect of privacy (by design) should not be disregarded. Even though the onboarding document per Appendix D emphasizes the permission system of least-privilege, documentation should be available regarding what kind of permissions exist, i.e., read/edit/contribute/delete rights and for which platforms those apply. It would also be beneficial to discuss whether documentation should be stored on a separate platform or if the current conditions, i.e., storing documents in the Cloudstore and Gitlab, is a good idea.

Especially in the area of health, self-harming behavior should not be underestimated. Hence, we have added more reasons as for what could trigger said behavior in Figure 4.14. The aspect of TOM which we described in Section 3.1.3 can also be used to evaluate which measures have already been put into place and which ones are still in development. By conducting a test intervention, we could see that the diversity of question types is highly developed. Interventions can contain question types such as:

- single/multiple choice
- sliders
- multimedia components (audio and video)

- etc.

According to the privacy policy, user data is used for scientific purposes by the Department of Clinical Psychology and Psychotherapy at the University of Ulm [71]. To ensure that data is collected accurately for study purposes, it may also be advantageous to regularly conduct risk assessments together with all parties involved, whenever a major version is released for eSano.

4.2.4 Applying the checklist on eSano

We have applied the three checklists in Figure 4.9, 4.10 and 4.11 respectively.

No.	Legal basis	Title	Legal obligation	Yes	No	In parts	Not relevant
1	• Art. **30** GDPR	• Records of processing activitities	Do the data controller and data processor maintain a record of processing activities?	☒	☐	☐	☐
2	• Art. **9(1)** GDPR	• Processing of special categories of personal data	Does the company process personal data?	☒	☐	☐	☐
3	• Art. **9(2)** GDPR	• Processing of special categories of personal data	Does the company process sensitive personal data?	☒	☐	☐	☐
4	• Art. **37** GDPR • Art. **39(1)(e)** GDPR • Section **38(1)** FDPA	• Designation of the data protection officer • Tasks of the data protection officer • Data protection officers of private bodies	Has a data protection officer been appointed?	☒	☐	☐	☐
5	• Art. **38** GDPR • Recital **97** • Section **6** FDPA	• Position of the data protection officer • Data Protection Officer • Position	Is the company informed about the rights of a data protection officer?	☒	☐	☐	☐
6	• Art. **28** GDPR • Art. **29** GDPR • Art. **32** GDPR	• Processor • Processing under the authority of the controller and processor • Security of processing	Has the task of data processing been transferred to a processor?	☒	☐	☐	☐
7	• Art. **35** GDPR • Recital **75**	• Data protection impact assessment • Risks to the Rights and Freedoms of Natural Persons	Is there a high risk to the rights and freedoms of users?	☒	☐	☐	☐
8	• Art. **35** GDPR • Art. **36(1)-(3)** GDPR • Recital **75** • Recital **90**	• Data protection impact assessment • Prior consultation • Risks to the Rights and Freedoms of Natural Persons	If No. 7 was answered with 'Yes', has a Data Protection Impact Assessment been carried out?	☐	☐	☒	☐
9	• Art. **4(12)** GDPR • Art. **33** GDPR • Art. **58(1)** GDPR • Recital **85** • Recital **87** • Section **42(4)** FDPA • Section **43(4)** FDPA	• Personal data breach • Notification of a personal data breach to the supervisory authority • Powers • Notification Obligation of Breaches to the Supervisory Authority • Promptness of Reporting/Notification • Penal Provisions • Provisions on administrative fines	In case of a personal data breach, does the company have right procedures in place to report, identify and investigate the breach?	☒	☐	☐	☐
10	• Art. **32** GDPR • Recital **83**	• Security of processing	Did the organization take appropriate Technical and Organizational Measures to ensure that data processing is secure?	☒	☐	☐	☐

Figure 4.15: Obligations of the data processor based on [70], [9] and [47] applied on eSano

No.	Legal basis	Title	Legal obligation	Yes	No	In parts	Not relevant
11	• Art. **6(1)(f)** GDPR • Art. **13** GDPR • Art. **22(1), 22(4)** GDPR • Art. **27** GDPR • Art. **44** GDPR • Art. **77** GDPR	• Lawfulness of processing • Information to be provided where personal data are collected from the data subject • Automated individual decision-making, including profiling • Representatives of controllers or processors not established in the Union • General principle for transfers • Right to lodge a complaint with a supervisory authority	Does the company know what information obligations they have, if (only) they process the collected user data?	☒	☐	☐	☐
12	• Art. **6(1)(f)** GDPR • Art. **13-22** GDPR • Art. **26(2)** GDPR • Art. **27** GDPR • Art. **44** GDPR • Art. **77** GDPR • Art. **89(1)** GDPR • Recital **60** • Recital **61** • Recital **62** • Section **29(1)** FDPA • Section **33** FDPA	• Lawfulness of processing • Joint controllers • Representatives of controllers [...] • General principle for transfers • Right to lodge a complaint [...] • Safeguards [...] • Information Obligation • Time of information • Exceptions to the Obligation to Provide Information • [...] secrecy obligations • Information to be provided where personal data have not been obtained from the data subject	Does the company know what information obligations they have, if user data has been processed by other organizations?	☒	☐	☐	☐
13	• Art. **5(2)** GDPR • Art. **12** GDPR • Art. **15** GDPR • Recital **63** • Recital **64** • Section **34(1)-(2)** FDPA	• Purpose limitation • Transparent information [...] • Right of access by the data subject • Right of access • Identity verification • Right of access by the data subject	Can the data controller provide information about the data it stores from users and are they capable of providing a copy of the data upon request?	☒	☐	☐	☐
14	• Art. **5(2)** GDPR • Art. **12(1), 12(3), 12(6)** • Art. **16** GDPR • Art. **19** GDPR	• Purpose limitation • Transparent information [...] • Right to rectification • Notification obligation [...]	Can the data controller correct inaccurate data?	☒	☐	☐	☐
15	• Art. **4(2)(e)** GDPR • Art. **5(1)(e)** GDPR • Art. **12** GDPR • Art. **17** GDPR • Art. **19** GDPR • Recital **26** • Recital **39** • Recital **65** • Recital **66** • Section **35** FDPA	• Definitions • Lawfulness, Fairness and transparency • Transparent information [...] • Right to erasure • [...] erasure of personal data [...] • Not Applicable to Anonymous Data • Principles of Data Processing • Right to Rectification and Erasure • Right to be Forgotten	Can the data controller delete data if relevant prerequisites are satisfied?	☒	☐	☐	☐
16	• Art. **12** GDPR • Art. **20** GDPR • Recital **68**	• Transparent information • Right to data portability • Right of Data Portability	Upon request, can the data controller provide data of a user in a machine-readable format which can then be used by another controller?	☐	☐	☒	☐
17	• Art. **12** GDPR • Art. **21** GDPR • Recital **70**	• Transparent information • Right to object • Right to Object to Direct Marketing	Does the company know what to do if data subjects objects to processing their data or profiling?	☒	☐	☐	☐

Figure 4.16: Information obligations and data subject rights based on [70], [9] and [47] applied on eSano

No.	Legal basis	Title	Legal obligation	Yes	No	In parts	Not relevant
18	• Art. **6(1)** GDPR • Art. **13** GDPR • Art. **14** GDPR • Art. **21(1)-(4)** • Art. **35(7)(a)** GDPR • Recital **47**	• Lawfulness of processing • Information to be provided where personal data are collected from the data subject • Information to be provided where personal data have not been obtained from the data subject • Right to object • Data protection impact assessment • Legitimate Interest	Does a legal basis exist for the processing of user data?	☒	☐	☐	☐
19	• Art. **6(1)** GDPR • Art. **7** GDPR • Art. **8** GDPR • Art. **9** GDPR • Recital **32** • Recital **42** • Recital **43** • Recital **171**	• Lawfulness of processing • Conditions for consent • Conditions applicable to child's consent in relation to information society serves • Processing of special categories of personal data • Conditions for Consent • Burden of Proof and Requirements for Consent • Freely Given Consent • Repeal of Directive 95/46/EC and Transitional Provisions	Can the institution ensure and prove that a data subject has given appropriate consent for data collection and processing?	☒	☐	☐	☐
20	• Art. **6(1)** GDPR • Art. **7** GDPR • Art. **13** GDPR • Art. **14** GDPR • Recital **32** • Recital **50** • Section **24** FDPA	• Lawfulness of processing • Conditions for consent • Information to be provided where personal data are collected from the data subject • Information to be provided where personal data have not been obtained from the data subject • Conditions for Consent • Further Processing of Personal Data • Processing for other purposes by private bodies	Does the company meet specific conditions if data is being processed for a reason other than the one for which they were collected?	☒	☐	☐	☐

Figure 4.17: Legal bases for processing based on [70], [9] and [47] applied on eSano

Many answers to questions stated in the “Legal obligation” column of the checklist can already be answered by information given in the privacy policy. The eSano platform processes sensitive personal data as it uses interventions to conduct studies [4]. Because of health data, there is a high risk for users which is why a DPIA is required as stated in Section 4.2.3. Some questions have also been clarified verbally with the eSano, i.e., the checkboxes that we marked as “in parts”. A DPIA has been conducted in parts. Documentation regarding risk assessments, data protection and requirements specification exist, but their contents could be described in more detail. In this case, it would be beneficial to evaluate whether each key point of Figure 3.5 has been fulfilled. If someone uses their right to data portability (question 16), the eSano team stated that data collected from users cannot just be given by clicking a button. Instead, the platform operator needs to look at specific parts of the platform to evaluate and collect the user data. As for question 19 in Figure 4.11, the institution asks users for written consent for the simple reason that conditions (such as the declaration of consent) vary, depending on each study.

4.3 Summary

In this chapter, we have put our research into practice. In the first part of this chapter we started by structuring our findings of previous chapters into a context that aligns with eHealth while we used the second part to apply said structures to eSano. We argue that in general, eSano is GDPR-compliant in almost all aspects. A thorough evaluation is not possible in the context of this thesis as it would require an in-depth examination of whether provided documentation and processes put in place align with specific laws. Since eSano is a work in progress, its privacy policy must be checked regularly and also adapted in the event of changes in the data management process. This is because new legal rulings and judgments in this regard regularly involve developments that must also be applied in the company's own data privacy statement. Thorough documentation for a DPIA is required and documentation regarding a risk assessment does not suffice if it is not constantly being updated. Despite room for improvement regarding documentation, our findings indicate a secure handling of user data and standards put into place to ensure compliance with not only the GDPR, but also other norms and laws.

5 Discussion

Chapter 5 discusses the ever-growing challenges of complying with legislation. We will also look at some aspects of the GDPR which have been criticized.

5.1 Challenges

By analyzing the GDPR in the context of eHealth in Chapters 3 and 4, we have become increasingly aware of the challenges businesses face. We will summarize some of them in this section.

5.1.1 Challenges of ensuring privacy-compliant health apps

The impact of the GDPR on the development of software harbors various risks and opportunities. Risks and disadvantages are:

- enormous costs to comply with regulation(s)
- lack of incentives due to over-regulation
- little room for maneuver to follow the laws
- massive fines in case of breaches

Opportunities and advantages include:

- standardization of laws among EU member states
- protection of user rights
- adaptive framework required for digitization
- increased cybersecurity

- exchange of (processed) data among several countries
- trust by customers due to accountability
- better understanding of collected data

Setting up and certifying a QMS dramatically increases the costs for manufacturers [49]. Smaller software producers such as startups or university spin-offs are particularly affected. The Johner Institute criticizes that eHealth producers have to deal with more than 600 pages of specifications related to data security, as we could see in Section 4.1.3, and these do not even include the GDPR [69]. They argue that more restrictions are unnecessary and that the infrastructure itself must be simplified. In fact, institutes are willing to comply with the GDPR, but a lack of resources, such as time and money, pose a significant hindrance to prioritizing it [72].

5.1.2 Issues of transferring data to other countries

As described in Section 2.2.1, SCC allow data transfer to other countries [33]. One major problem is that they are impractical for transferring data to US government entities or universities. This is because the US states each have their own different laws regarding data protection (see Section 2.1.2). Despite the GDPR allowing businesses to process personal data for scientific research purposes, each country has several legal restrictions in place that must be complied with.

Pseudonymized personal data can be used for international data transfer, but it falls under the category personal data, implying that compliance with the GDPR is obligatory [73]. Rarely, one could anonymize the data, but that may render the data useless. The authors of the paper argue that the issue of transferring data to countries outside the EEA must be addressed as science requires global collaboration. In Section 2.1.2 we have mentioned the EU-US Privacy Shield. The reason for its invalidity is that data transfer would violate rights defined in the Charter of Fundamental Rights of the European Union. New technology and encryption schemes could provide new opportunities of protecting data, but do not avoid the problem of transferring data. Countries in the EEA are cooperating with the US National Institutes of Health (NIH) in approximately 5000 studies, but a non-significant amount of them get cancelled due to legal reasons. The deficiency of best-practices worldwide to protect data makes it more difficult to share large data sets [74]. To tackle the challenges outlined here, the authors propose that the EU must urge other countries for changes in their regulations or the potential of research may not be fully unfolded.

5.2 Criticism

Even though the European Commission created an eHealth Action Plan for the years 2012 – 2020, the findings of that plan have not been cleared until now [25]. One of the most significant issues is still the cost factor, especially for startups, which gets amplified by the fact that there are legal limitations as to which extent data collected by eHealth and mHealth apps can be used.

5.2.1 Complexity, time investment, and obscurity

Every so often, the EDPB has to assert the meaning of specific terms even though it is the recitals that aim to improve understanding of the GDPR [75]. For instance, the term “scientific research” refers to gaining new insights, but the EDPB had to clarify that said research must be related to projects that maintain methodological guidelines. Although the GDPR aims to bring conformity for each member state, there are inconsistencies caused by national legislation provisions that exacerbate data exchange. The paper also exemplifies that the length and technical language of privacy policies causes users to refrain from reading them in the first place. Even when people are provided with all the information they need, they still require skills to understand and apply them. If an mHealth app were to collect personal data from users automatically, Art. 13 of the GDPR would apply [9] according to the EDPB [75], but that still puts the user at risk of not being informed about what data the device transmits. Data subjects are informed about their rights in Art. 13 and 14 GDPR [9], but they do not have to be briefed on Art. 22(3) GDPR, which allows them to reveal their stance and to contest automated processing [75].

A paper published by the Yearbook of Medical Informatics argues that getting (explicit) user consent is inappropriate [74]. They claim that it is uncommon for every involved party to get contacted in case the collected data serves another purpose apart from its original one. Using “public interest” as a legal basis is also objectionable since the term is interpreted differently among members of the EU. Nonetheless, the authors are aware that this room for interpretation is necessary to allow organizations to comply with other regulations in their country. Regarding transferring data to third countries, the authors consider the processes to be too complicated in practice. Reasons for this are that each user would have to be informed about the transfer and rather pointless SCC, which the US cannot agree upon. Nevertheless, high standards could also be seen as a blessing in disguise: innovation in situations which are characterized

by a pressure in time could lead to development of solutions unfit for data protection [74].

Roughly 86 percent of the 862 companies surveyed claim that the GDPR is detrimental to their competitive position [76]. The information service of the Institute of the German Economy iwd surveyed 293 companies in 2019 as to why they see downsides in the GDPR.

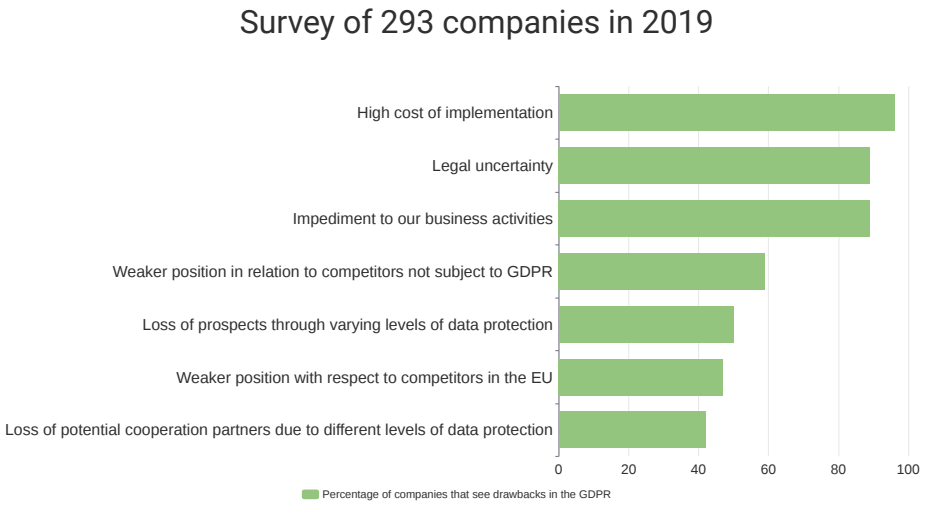


Figure 5.1: GDPR imposing a high burden on companies based on [76]

Figure 5.1 illustrates that almost every company in the survey thinks that the implementation of the GDPR comes with a high cost. Nearly the same amount criticizes the incertitude with regard to its legal basis and considers the GDPR to be a hindrance to business activities. Half of the people surveyed emphasize a competitive disadvantage.

5.2.2 Fines and data breaches

Another issue is that DPAs enforce fines on companies, even though the EU does not provide a consistent framework for archiving and cataloging purposes [77]. A recent study on data breaches concluded that Art. 5, 6, and 32 were most commonly referred to in terms of law enforcement [77]. On top of that,

the amount of the fine did not differ too much depending on the articles stated above.

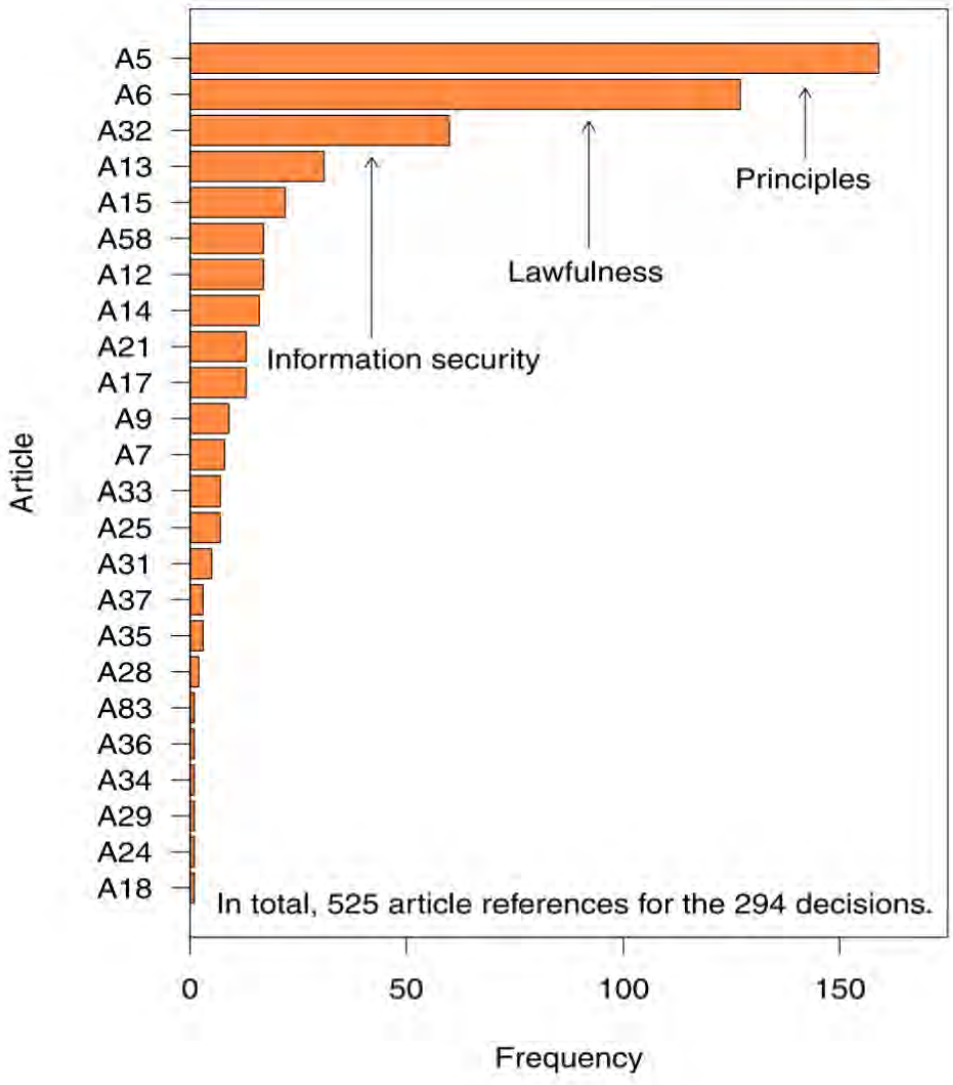


Figure 5.2: Articles referenced in enforcement cases from [77]. The usage of this chart has been approved from the original author

We can clearly see that the most crucial articles, i.e., 5, 6, and 32 are referenced by as much as 67 percent of enforcement-related cases. The subsequent Art. 13 and 15 of the GDPR are closely related to information obligations regarding data processing, while the other articles (5, 6, and 32) specifically address how personal data must be handled. Even the duty to appoint a DPO per Art. 37 of the GDPR, or to implement a DPIA according to Art. 35 GDPR proves that

some institutions are unwilling to cooperate with authorities [9]. Fines related to Art. 35-37 essentially show that the full context of the GDPR steadily impacts the development of software with the help of DPO's.

In addition, Germany does not clarify the meaning of "scientific research", wherefore other administrative bodies set up limits [53]. Since member states of the EU handle the range of scientific research differently, administrative barriers may pose a problem as health software will have different requirements depending on the member state they are developed in.

As stated in Section 3.1.5, data breaches can lead to remarkably high fines. A survey where companies[1] participated in 2018 made the vast difference in penalties even more explicit: while one company should (hypothetically) pay a fine of 1.7 billion euros, another organization would only have to pay 400 euros. Figure 5.1 concluded that Art. 5-6 GDPR were primarily responsible for enforcement-related cases [77]. Another (independent) study came to the same result:

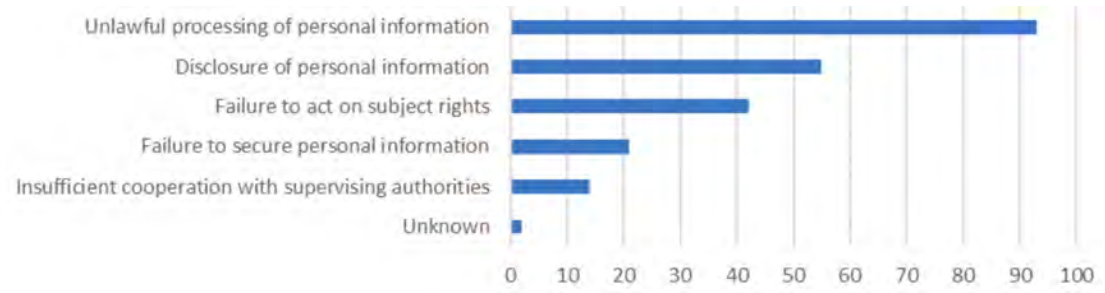


Figure 5.3: Clustering of 277 sanctions since March 31, 2020 from [72]

Figure 5.3 shows that companies were penalized for complying with the law with regard to data processing. Moreover, failing to disclose user data accounted for more than 50 sanctions. This tells us that these issues could have been prevented if the respective entities had spent time and effort complying with the GDPR.

5.3 Summary

We have shortly discussed how the implementation of the GDPR affects those who need to comply with it. On the one hand, the GDPR as a uniform and legal

[1] n = 62.

framework enables a high standard of data protection among more than 400 million citizens. On the other hand, we get a high level of legal uncertainty as individual countries often interpret the rules differently, which is aggravated by new data protection rules and norms. Depending on the point of view, one could argue that the GDPR allows users to have more trust into companies that protect their data, or one could see it as a disadvantage, especially if a business has to suffer greater expense than its competitors.

6 Conclusion

To comply with the aspects and requirements of IT security in the field of eHealth, various security precautions must be adopted. Therefore, it is essential for providers to familiarize themselves with standards and regulations and to take their implementation into account even before starting to develop health software. We will shortly summarize our findings and give an outlook for the future in this chapter.

6.1 Roundup

To understand the scope of the GDPR, we have looked at its history and relevance in the health sector. Due to ever-changing developments in technology, various security precautions must be taken to comply with the aspects and requirements of IT security in eHealth. If the prerequisites of the GDPR are ignored, confidential medical data may be lost or passed onto uninvolved third parties. This may also result in considerable permanent damage to the provider's image of an eHealth application, wherefore risk and incident management are essential to ensure the quality of an eHealth application. We have analyzed relevant articles of GDPR in the context of health software development and also addressed best practices on how compliance can be achieved. When analyzing the interface with other regulations, we noted that the GDPR must be used as a foundation on top of other ones, such as the MDR. Applying our findings onto eSano was not as difficult as we initially expected. This might be because of putting everything together in the first part of Chapter 4. What also helped is that the platform with its functionalities are well documented. We came to the conclusion that the GDPR is effective to protect health data of users and that more international collaboration is required to facilitate the process of sharing data for scientific purposes.

6.2 Outlook

As the proverb goes, “prevention is better than cure”, we can apply the same analogy to software development by arguing that compliance is a lot easier when considering everything before facing difficulties or breaches. It is reasonable to think that the idea behind the GDPR is a step in the right direction since it leads to more order and structure, but the execution of said idea needs improvement. Most of the people who use the internet simply could not be bothered about reading the privacy policy of each page they visit. However, the GDPR forces platform operators to become more responsible for their respective audience. Responsibility comes with accountability, and companies who do process sensitive health data should be held accountable. The GDPR has a strong impact on this aspect, and other regulations do as well. Even though cautiousness is always a prerequisite for processing (sensitive) personal data, we have discovered that Germany is a pioneer in using laws that the GDPR permits it to do so. For the sake of science and health, we hope that organizations use and exchange data if the laws allow it, not only for health research, but also to remain competitive in the health sector of Europe.

Bibliography

[1] L. Specht-Riemenschneider and A. Radbruch, “Datennutzung und -schutz in der Medizin: Forschung braucht Daten,” Deutsches Ärzteblatt, vol. 118, no. 27-28, 12-Jul-2021.

[2] “Entwicklungsgeschichte der Datenschutz-Grundverordnung,” European Data Protection Supervisor. [Online]. Available: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_de. [Accessed: 28-Jan-2022].

[3] “E-Health,” 24-Jan-2022. [Online]. Available: https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health.html. [Accessed: 20-May-2022].

[4] Kraft, R., Idrees, A. R., Stenzel, L., Nguyen, T., Reichert, M., Pryss, R., & Baumeister, H. (2021). eSano - An eHealth Platform for Internet- and Mobile-based Interventions. Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference, 2021, 1997–2002. https://doi.org/10.1109/EMBC46164.2021.9629534.

[5] E-Health – Digitalisierung im Gesundheitswesen, 14-Dec-2021. [Online]. Available: https://www.bundesgesundheitsministerium.de/e-health-initiative.html. [Accessed: 14-Jan-2022].

[6] Von K. Ruhenstroth, “Digitale Gesundheit: Herausforderungen für den patientendatenschutz,” Dr. Datenschutz, 21-Aug-2019. [Online]. Available: https://www.dr-datenschutz.de/digitale-gesundheit-herausforderungen-fuer-den-patientendatenschutz/. [Accessed: 19-Dec-2021].

[7] “76% of users ignore cookie banners!,” Amazee Metrics, 26-Sep-2019. [Online]. Available: https://www.amazeemetrics.com/en/blog/76-ignore-cookie-banners-the-user-behavior-after-30-days-of-gdpr/. [Accessed: 20-Dec-2021].

[8] “Entwicklungsgeschichte der Datenschutz-Grundverordnung,” European Data Protection Supervisor. [Online]. Available: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_de. [Accessed: 26-Feb-2022].

[9] “General Data Protection Regulation,” General Data Protection Regulation (GDPR), 02-Sep-2019. [Online]. Available: https://gdpr-info.eu/ [Accessed: 10-Feb-2022].

[10] “A brief history of data protection: How did it all start?,” EuroCloud Trusted Digital Competence Platform, 01-Jun-2018. [Online]. Available: https://eurocloud.org/news/article/a-brief-history-of-data-protection-how-did-it-all-start/. [Accessed: 03-Feb-2022].

[11] M. Hillenbrand and N. *, “Geschichte des Datenschutz,” Verband Datenschutz und Digitalisierung, 18-May-2021. [Online]. Available: https://www.vdaten.de/2021/02/18/geschichte-des-datenschutz/. [Accessed: 20-Feb-2022].

[12] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, DSGVO – BDSG Texte und Erläuterungen. Appel & Klinger Druck und Medien GmbH, Bonn, 2020.

[13] Archick, K. (2021). U.S.-EU Privacy Shield and Transatlantic Data Flows (CRS Report No. R46917). Retrieved from Congressional Research Service website: https://crsreports.congress.gov/product/pdf/R/R46917.

[14] Overview – Data Protection and the EU. [Online]. Available: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/. [Accessed: 27-Feb-2022].

[15] Barker, Tyson. (2020). BREAKING THE TRANSATLANTIC DATA TRILEMMA The EU Must Step Up Its Approach to EU-US Data Flows (Policy brief 27). [Online]. Available: https://dgap.org/en/research/publications/breaking-transatlantic-data-trilemma. [Accessed: 15-May-2022].

[16] C. Maag, Neues Schweizer Datenschutzgesetz kommt erst 2023, 08-Mar-2022. [Online]. Available: https://www.computerworld.ch/security/datenschutz/neues-schweizer-datenschutzgesetz-kommt-2023-2747442.html. [Accessed: 10-Mar-2022].

[17] M. Schrems, “The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield ,” 16-Jul-2020. [Online]. Available: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf. [Accessed: 07-May-2022].

[18] “Data Privacy Laws by State: Comparison Charts,” Bloomberg Law, 02-Feb-2022. [Online]. Available: https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/. [Accessed: 28-Feb-2022].

[19] D. Reinsch, “IEC 82304 – Was die Norm zu „Health Software‘ fordert,” Johner Institut, 14-Sep-2016. [Online]. Available: https://www.johner-

institut.de/blog/iec-62304-medizinische-software/iec-82304/. [Accessed: 18-Apr-2022].

[20] T. Ü. V. Rheinland, EU-Medizinprodukteverordnung MDR 2017/745. [Online]. Available: https://www.tuv.com/germany/de/eu-medizinprodukteverordnung-mdr-2017-745.html [Accessed: 15-Apr-2022].

[21] Health Insurance Portability and Accountability Act [HIPAA] of 1996, Pub. L. No. 104-191.

[22] S. O'Connor, R. Nurwono, A. Siebel, and E. Birrell, "(Un)clear and (in)conspicuous: The right to opt-out of sale under CCPA," arXiv.org, 14-Jul-2021. [Online]. Available: https://arxiv.org/abs/2009.07884. [Accessed: 13-Mar-2022].

[23] "California Privacy Rights Act: An overview," Privacy Rights Clearinghouse, 10-Mar-2020. [Online]. Available: https://privacyrights.org/resources/california-privacy-rights-act-overview. [Accessed: 15-Mar-2022].

[24] D. Koevoets, "The Influence of Article 89 GDPR on the Use of Big Data Analytics for the Purpose of Scientific Research," thesis, 2017.

[25] A. Singhal and M. Cowie, "What is e-Health?," e-Journal of Cardiology Practice, vol. 18, no. 24, Jun. 2020.

[26] ALLEA (European Federation of Academies of Sciences and Humanities), FEAM (Federation of European Academies of Medicine), und EASAC (European Academies' Science Advisory Council), International Sharing of Personal Health Data for Research. DE: ALLEA, 2021. doi: 10.26356/IHDT.

[27] F. Blachetta, et al., Weiterentwicklung der eHealth-Strategie: Studie im Auftrag des Bundesministeriums für Gesundheit, Berlin: BMG, 2016.

[28] "Die wichtigsten Vorteile," SERIE: DIE CHANCEN VON E-HEALTH. [Online]. Available: https://www.triumph-adler.at/talking-future/e-health-serie-teil-4-. [Accessed: 20-Feb-2022].

[29] C. Bauer, M. Breuer, D. Diebold, F. Eickmeier, J. Klekamp, S. A. Maucher, M. Neuber, G. Rackwitz, and T. Wegmann, "Browser-cookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte," 08-Oct-2015. [Online]. Available: https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf. [Accessed: 20-Apr-2022].

[30] E. A. Salami, “An Analysis of the General Data Protection Regulation (EU) 2016/679,” SSRN Electronic Journal. Elsevier BV, 2017. doi: 10.2139/ssrn.2966210.

[31] T. Niebler, T. Zerres, und C. Zerres, „Datenschutzrechtlicher Rahmen von E-Health in Deutschland“, Arbeitspapiere für Marketing und Management; 54, 2021, doi:10.48584/OPUS-4989.

[32] Consumers, Health, Agriculture and Food Executive Agency., Assessment of the EU Member States’ rules on health data in the light of GDPR. LU: Publications Office, 2021. doi: 10.2818/546193.

[33] D. Peloquin, M. DiMaio, B. Bierer, and M. Barnes, “Disruptive and avoidable: GDPR challenges to secondary research uses of data,” European Journal of Human Genetics, vol. 28, no. 6. Springer Science and Business Media LLC, pp. 697–705, Mar. 02, 2020. doi: 10.1038/s41431-020-0596-x.

[34] Orientierungshilfe zum Gesundheitsdatenschutz.: Bundesministerium für Wirtschaft und Energie, Berlin, 2018.

[35] N. Leistner, “Digitale Medizinprodukte,” MEC//ABC Ihr Lotse zu klinischen Daten, 29-Nov-2020. [Online]. Available: https://mec-abc.de/newsletter-11-2020/. [Accessed: 23-Apr-2022].

[36] A.-R. Laireiter and U. Willutzki, “Internet-basierte psychologische Intervention Unterstützung der Psychotherapie,” Deutsches Ärzteblatt, vol. 10, no. 19-30, Oct-2003.

[37] E. Mougiakou and M. Virvou, “Based on GDPR privacy in UML: Case of e-learning program.,” in IISA, 2017, pp. 1–8.

[38] J. Tom, E. Sing, and R. Matulevičius, „Conceptual Representation of the GDPR: Model and Application Directions“, Lecture Notes in Business Information Processing. Springer International Publishing, S. 18–28, 2018. doi: 10.1007/978-3-319-99951-7_2.

[39] D. M. Huth, “Development of a reference process model for GDPR compliance management based on enterprise architecture,” dissertation, 2021.

[40] D. Barrett and R. E. Silverman, SSH the secure shell: The definitive guide. Sebastopol, CA: O’Reilly Media, 2001.

[41] P. Patil, P. Narayankar, Narayan D.G., und Meena S.M., „A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish“, Procedia Computer Science, Bd. 78. Elsevier BV, S. 617–624, 2016. doi: 10.1016/j.procs.2016.02.108.

[42] C. Bertram, “Anonymisierung und Pseudonymisierung,” Health IT & Medizintechnik Anonymisierung und Pseudonymisierung, 07-Oct-2021. [Online]. Available: https://www.johner-institut.de/blog/medizinische-informatik/anonymisierung-und-pseudonymisierung/. [Accessed: 08-Apr-2022].

[43] “Software & IEC 62304,” Johner Institut. [Online]. Available: https://www.johner-institut.de/blog/category/iec-62304-medizinische-software/. [Accessed: 28-Feb-2022].

[44] N. Martin, M. Friedewald, I. Schiering, B. A. Mester, D. Hallinan, and M. Jensen, DIE DATENSCHUTZ-FOLGENABSCHÄTZUNG NACH ART. 35 DSGVO Ein Handbuch für die Praxis. Stuttgart: Fraunhofer Verlag, 2020.

[45] G. Chassang, „The impact of the EU general data protection regulation on scientific research“, ecancermedicalscience, Bd. 11. Ecancer Global Foundation, Jan. 03, 2017. doi:10.3332/ecancer.2017.709.

[46] European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995, available at: https://www.refworld.org/docid/3ddcc1c74.html. [Accessed: 18-Apr-2022].

[47] Bundesdatenschutzgesetz [Online]. Available: https://www.gesetze-im-internet.de/englisch_bdsg/ [Accessed: 04-Apr-2022].

[48] “Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates,” EUR-Lex Access to European Union law. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R0745. [Accessed: 03-Apr-2022].

[49] M. Gerhard, “MDR regel 11: Der Klassifizierungs-Albtraum?,” 11-Oct-2021. [Online]. Available: https://www.johner-institut.de/blog/regulatory-affairs/mdr-regel-11/. [Accessed: 25-Apr-2022].

[50] “MDCG 2021-24 guidance on classification of Medical Devices,” Oct-2021. [Online]. Available: https://ec.europa.eu/health/system/files/2021-10/mdcg_2021-24_en_0.pdf. [Accessed: 16-May-2022].

[51] L. Salvatore, “IMDRF: Neues vom International Medical Device Regulators Forum,” Johner Institut, 04-May-2020. [Online]. Available: https://www.johner-institut.de/blog/qualitaetsmanagement-iso-

13485/imdrf-klassifizierung-von-risiken-durch-software-as-a-medical-device/ [Accessed: 20-Apr-2022].

[52] K. van der Sluijs, “MDR Guide for Medical Device Software,” 16-Jul-2021. [Online]. Available: https://www.fme.nl/system/files/publicaties/2021-09/MDR%20Guide.pdf. [Accessed: 25-May-2022].

[53] J. Meszaros, M. C. Compagnucci, und T. Minssen, „The Interaction of the Medical Device Regulation and the GDPR“, The Future of Medical Device Regulation. Cambridge University Press, S. 77–90, Apr. 07, 2022. doi: 10.1017/9781108975452.007.

[54] Struktur Technische Dokumentation (Medizinprodukte), Aug-2021. [Online]. Available: https://www.mdc-ce.de/fileadmin/user_upload/Downloads/mdc-Dokumente/Formulare_Recommend/2385_d_Struktur_Technische_Dokumentation_Medizinprodukte.pdf. [Accessed: 26-Apr-2022].

[55] C. Isele, P. Kaufmann, D. Koeppe, C. Neumann, T. Schütz, B. Schütze, and G. Spyra, “Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO),” 28-Apr-2018. [Online]. Available: https://www.gesundheitsdatenschutz.org/download/privacy-design-default.pdf. [Accessed: 22-May-2022].

[56] Bürgerliches Gesetzbuch. [Online]. Available: https://www.gesetze-im-internet.de/bgb/. [Accessed: 13-May-2022].

[57] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,” The TQM Journal, vol. 33, no. 7. Emerald, pp. 76–105, Mar. 16, 2021. doi: 10.1108/tqm-09-2020-0202.

[58] K. Schnetter, “ISO 27001: IT-Sicherheitsmanagement für alle Medizinproduktehersteller?,” 20-Oct-2020. [Online]. Available: https://www.johner-institut.de/blog/iec-62304-medizinische-software/iso-27001/. [Accessed: 08-Jun-2022].

[59] “DSGVO: Leitlinien, Empfehlungen, Bewährte Verfahren,” edpb European Data Protection Board. [Online]. Available: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de. [Accessed: 19-Apr-2022].

[60] H. Koch, B. Schütze, G. Spyra, and M. Wefer, “Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO),” 15-May-2017. [Online]. Available: https://www.medizin.uni-kiel.de/de/fakultaet/dateien-

fakultaet/datenschutzrechtliche-anforderungen-an-die-medizinische-forschung. [Accessed: 23-Apr-2022].

[61] A. Backer-Heuveldop, S. Gindera, C. Isele, D. Koeppe, M. Letter, J. Mönter, J. Schlütter, and D. B. Schütze, "Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen," Leitfaden fu r die Erstellung von Löschkonzepten im Gesundheitswesen. [Online]. Available: https://www.gesundheitsdatenschutz.org/download/loeschkonzept_leitfaden.pdf. [Accessed: 20-Apr-2022].

[62] S. Siebert, "DSGVO-Konforme Datenschutzerklärung ," eRecht24, 07-Apr-2022. [Online]. Available: https://www.e-recht24.de/muster-datenschutzerklaerung.html. [Accessed: 26-Mar-2022].

[63] R. Koch, "Cookies, the GDPR, and the ePrivacy directive," 09-May-2019. [Online]. Available: https://gdpr.eu/cookies [Accessed: 10-May-2022].

[64] "Das Recht auf Löschung (Vergessenwerden) Einfach Erklärt," Das Recht auf Löschung (Vergessenwerden) einfach erklärt, 05-Apr-2022. [Online]. Available: https://www.dr-datenschutz.de/das-recht-auf-loeschung-vergessenwerden-einfach-erklaert/. [Accessed: 22-Jun-2022].

[65] "For how long can data be kept and is it necessary to update it?," 13-Dec-2019. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en. [Accessed: 21-Jun-2022].

[66] V. Hammer, „DIN 66398", Datenschutz und Datensicherheit - DuD, Bd. 40, Nr. 8. Springer Science and Business Media LLC, S. 528–533, Juli 22, 2016. doi: 10.1007/s11623-016-0651-5.

[67] "Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen," Unabhängiges Landeszentrum für Datenschutz, 07-May-2018. [Online]. Available: https://www.datenschutzzentrum.de/artikel/1225-Kurzpapier-Nr.-18-Risiko-fuer-die-Rechte-und-Freiheiten-natuerlicher-Personen.html. [Accessed: 20-Apr-2022].

[68] B. Yuan and J. Li, "The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation," International Journal of Environmental Research and Public Health, vol. 16, no. 6. MDPI AG, p. 1070, Mar. 25, 2019. doi: 10.3390/ijerph16061070.

[69] A. Schulze, "Wie Sie die Anforderungen an die Datensicherheit und den Datenschutz für DIGA erfüllen," 08-Feb-2021. [Online]. Avail-

able: https://www.johner-institut.de/blog/regulatory-affairs/datensicherheit-und-datenschutz-fuer-diga/. [Accessed: 10-May-2022].

[70] Checkliste und Merkblätter zur Datenschutzgrundverordnung, Feb-2018. [Online]. Available: https://www.ehdv.de/wp-content/uploads/sites/7/2018/04/Checkliste-und-Merkbl%C3%A4tter-zur-Datenschutzgrundverordnung.pdf. [Accessed: 19-May-2022].

[71] "Informationen zum Datenschutz," eSano online-trainings. [Online]. Available: https://patient.dev.aas2.klips.ifp.uni-ulm.de/privacy. [Accessed: 10-Jun-2022].

[72] W. Presthus and K. F. Sønslien, "An analysis of violations and sanctions following the GDPR," International Journal of Information Systems and Project Management, vol. 9, no. 1. pp. 38–53, Sep. 16, 2021. doi: 10.12821/ijispm090102.

[73] H. B. Bentzen, R. Castro, R. Fears, G. Griffin, V. ter Meulen, and G. Ursin, "Remove obstacles to sharing health data with researchers outside of the European Union," Nature Medicine, vol. 27, no. 8. Springer Science and Business Media LLC, pp. 1329–1333, Aug. 2021. doi: 10.1038/s41591-021-01460-0.

[74] M. Christofidou, N. Lea, and P. Coorevits, "A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis," Yearbook of Medical Informatics, vol. 30, no. 01. Georg Thieme Verlag KG, pp. 226–232, Aug. 2021. doi:10.1055/s-0041-1726512.

[75] R. Ducato, "Data protection, scientific research, and the role of information," Computer Law Security Review, vol. 37. Elsevier BV, p. 105412, Jul. 2020. doi: 10.1016/j.clsr.2020.105412.

[76] B. Engels, "Datenschutz: Ungeliebtes Regelwerk," iwd Der Informationsdienst des Instituts der deutschen Wirtschaft, 21-Jan-2020. [Online]. Available: https://www.iwd.de/artikel/datenschutz-ungeliebtes-regelwerk-456328/. [Accessed: 10-Jun-2022].

[77] J. Ruohonen und K. Hjerppe, „The GDPR enforcement fines at glance", Information Systems, Bd. 106. Elsevier BV, S. 101876, Mai 2022. doi: 10.1016/j.is.2021.101876.

A Acronyms

BCR	Binding Corporate Rules
CCPA	California Consumer Privacy Act
CMS	Content Management System
CPOE	Computerized Physician Order Entry
CPRA	California Privacy Rights Act
DIN	German Institute for Standardization
DPA	Data Protection Authority
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DPMS	Data Protection Management System
DPO	Data Protection Officer
EDPB	European Data Protection Board
EU	European Union
EEA	European Economic Area
FDPA	Federal Data Protection Act
FDA	Food and Drug Administration
FMG	Federal Ministry of Health
GAMP	Good Automated Manufacturing Practice
GCC	German Civil Code
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IMDRF	International Medical Device Regulators Forum
IMI	Internet- and mobile-based intervention
ISMS	Information Security Management System
ISO	International Organization for Standardization
KPI	Key-Performance-Indicator
MDCG	Medical Device Coordination Group
MDR	Medical Device Regulation
NIH	National Institutes of Health
PDCA	Plan-Do-Check-Act
QMS	Quality Management System
ROPA	Records of Processing Activities
SCC	Standard Contractual Clauses
SPM	Standard Data Protection Model
SPoC	Single Point of Contact
TOM	Technical and Organizational Measures

B Declaration of consent

Datenschutzrechtliche Aufklärung und
Einwilligung für Patient:innen
Version 1.1 eingereicht bei der Ethikkommission der DGPs am 29.07.2020
und sprachlich finalisiert am 19.10.2020
Universität Ulm
Prof. Dr. Harald Baumeister
Friedrich-Alexander-Universität Erlangen-Nürnberg
Prof. Dr. Matthias Berking
Assoc. Prof. Dr. David Daniel Ebert
Ansprechpartnerin für eventuelle Rückfragen:
Dr. Anna-Carlotta Zarski
Friedrich-Alexander-Universität Erlangen-Nürnberg
E-Mail: evaluation@psychonlinetherapie.de
Telefon: +49-(0)9131/85 67570

ulm university universität ulm

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

Datenschutzrechtliche Aufklärung und Einwilligung gem. Art. 13 EU-DSGVO
Universität Ulm und Friedrich-Alexander-Universität Erlangen-Nürnberg

Titel der Studie:

PSYCHOnlineTHERAPIE

INTEGRATION VON ONLINE-INTERVENTIONEN IN DIE AMBULANTE PSYCHOTHERAPIE BEI PATIENT:INNEN MIT DEPRESSIVEN STÖRUNGEN UND ANGSTSTÖRUNGEN

....
Name der einwilligenden Person in Druckbuchstaben Geburtsdatum

Versichert bei
- ☐ AOK Baden-Württemberg
- ☐ Bosch BKK

.....
Versichertennummer

....
E-Mail-Adresse Telefonnummer

Kontodaten (für Überweisung der Aufwandsentschädigung):

Kreditinstitut: .....

BIC: .....

IBAN: .....

1. Ausführliche Beschreibung des Forschungsvorhabens

Im Rahmen der Studie PSYCHOnlineTHERAPIE wird untersucht ob zwei Studienbedingungen *verzahnter Psychotherapie* (PSYCHOnlineTHERAPIE$_{fix}$ und PSYCHOnlineTHERAPIE$_{flex}$) ebenso wirksam wie die ambulante psychotherapeutische Routineversorgung im Rahmen des FacharztProgramms der AOK BW oder des Facharztprogramms der BOSCH BKK (PSYCHOnlineTHERAPIE$_{standard}$) sind. Unter Routineversorgung wird die Versorgung im Sinne der psychotherapeutischen Einzelleistung im Rahmen des Selektivvertrags zur Versorgung in den Fachgebieten der Neurologie, Psychiatrie, Psychosomatik und Psychotherapie (PNP-Selektivvertrag) gemäß § 73c SGB V verstanden, die vor Ort oder videobasiert durchführbar ist. *Verzahnte Psychotherapie* bedeutet, dass in diesen beiden Studienbedingungen (PSYCHOnlineTHERAPIE$_{fix}$ und PSYCHOnlineTHERAPIE$_{flex}$) ein Teil der Psychotherapiesitzungen gemäß der Routineversorgung durch selbstständig zu bearbeitende Online-Sitzungen ersetzt wird. Zudem möchten wir die Kosten-Effektivität dieser beiden Studienbedingungen gegenüber der Routineversorgung untersuchen und ihre Akzeptanz, Durchführbarkeit und Verbesserungsmöglichkeiten erfassen. Außerdem interessieren wir uns für Faktoren, die den Therapieerfolg beeinflussen, sowie mögliche Risiken und Nebenwirkungen. Teilnehmende Patient:innen haben damit die Möglichkeit, je nach Gruppenzugehörigkeit einen innovativen und neuen Therapieansatz kennenzulernen, der in einigen Studien bereits seine Wirksamkeit bewiesen hat. Nähere Informationen zum Forschungsvorhaben können der Teilnahmeinformation entnommen werden. PSYCHOnlineTHERAPIE wird im Rahmen des Innovationsfonds nach § 92 Abs. 1 SGB V (Förderkennzeichen: 01NVF18036) gefördert.

2. Inhalt und Zweck der Studie

Die Studie PSYCHOnlineTHERAPIE zielt darauf ab, die ambulante psychotherapeutische Routineversorgung nachhaltig zu flexibilisieren und zu digitalisieren. Das Potenzial internet- und mobile-basierter Interventionen (IMIs) soll angesichts der mittlerweile sehr umfangreichen und vielversprechenden Forschungsergebnisse genutzt und ausgeschöpft werden. Insgesamt gibt es drei Studienbedingungen: PSYCHOnlineTHERAPIE$_{fix}$, PSYCHOnlineTHERAPIE$_{flex}$ und PSYCHOnlineTHERAPIE$_{standard}$. Jede:r Therapeut:in ist einer der Studienbedingungen zugeteilt und die jeweiligen Patient:innen erhalten die entsprechende Behandlung.

In den Studienbedingungen PSYCHOnlineTHERAPIE$_{fix}$ und PSYCHOnlineTHERAPIE$_{flex}$ werden teilnehmenden Patient:innen von ihren Therapeut:innen individualisierte Online-Sitzungen angeboten: In der Studienbedingung PSYCHOnlineTHERAPIE$_{fix}$ erhalten Patient:innen genau 8 Psychotherapiesitzungen gemäß Routineversorgung und 8 Online-Sitzungen, in der Studienbedingung PSYCHOnlineTHERAPIE$_{flex}$ ist die Aufteilung der Sitzungen in Behandlungssitzungen gemäß der Routineversorgung und Online-Sitzungen den Therapeut:innen und Patient:innen überlassen. Teilnehmende Patient:innen der Studienbedingung PSYCHOnlineTHERAPIE$_{standard}$ erhalten kognitive Verhaltenstherapie, wie sie in der entsprechenden ambulanten psychotherapeutischen Routineversorgung üblich ist.

Im Rahmen der Studie erfolgt die Erhebung von Daten zu Studieneinschluss sowie 6, 12, 18 und 24 Wochen nach Einschluss in die Studie sowie ggf. 12 und 24 Monate nach Studieneinschluss durch online-basierte Fragebögen. Zusätzliche Daten werden im Rahmen von Telefon-/Videointerviews von Patient:innen und Therapeut:innen sowie durch pseudonymisierte Routinedaten durch die Krankenkassen erfasst. Weitere Informationen hierzu unter *4. Zu erhebende Daten*.

3. Betroffener Personenkreis

Zur Studie PSYCHOnlineTHERAPIE werden niedergelassene verhaltenstherapeutisch arbeitende Therapeut:innen in Baden-Württemberg, die selektivvertraglich angebunden sind, und ihre Patient:innen mit depressiven Erkrankungen und Angsterkrankungen zugelassen. Teilnehmende Patient:innen müssen folgende Voraussetzungen erfüllen, um an der Studie teilnehmen zu können:

- Mindestens 18 Jahre alt
- Diagnose einer depressiven Erkrankung und/oder Angsterkrankung (ICD-Liste PNP-Selektivvertrag)
- Versicherte der AOK Baden-Württemberg nehmen am FacharztProgramm der AOK Baden-Württemberg teil bzw. schreiben sich zeitgleich mit der Einschreibung in PSYCHOnlineTHERAPIE in dieses ein, sofern die Voraussetzungen zur Sofortabrechnung (SANE) vorliegen
- Versicherte der Bosch BKK nehmen am Facharztprogramm der Bosch BKK teil bzw. schreiben sich zeitgleich mit der Einschreibung in PSYCHOnlineTHERAPIE in dieses ein, sofern die Voraussetzungen zur Sofortabrechnung (SANE) vorliegen
- Teilnahme an einer Eingangsbefragung (Online-Befragung und Telefon-/Videointerview)
- Vorhandensein eines Internetzugangs sowie eines internetfähigen Endgerätes (PC/Laptop/Smartphone/Tablet)
- Ausreichende Deutschkenntnisse (Wort und Schrift)

Eine komorbide Diagnose im Bereich ICD-10-F2 (Schizophrenie, schizotype und wahnhafte Störungen) ist ein Ausschlusskriterium. Die Entscheidung über die klinische Eignung für die Studie trifft die:der jeweilige Therapeut:in. Teilnehmende Patient:innen müssen darüber hinaus die vorliegende Einwilligungserklärung unterschreiben. Zu weiteren Personenkreisen werden keine Informationen erhoben.

4. Zu erhebende Daten

Mittels Online-Befragungen werden neben soziodemographischen Daten (Geschlecht, Alter, Bildungsgrad, Größe, Gewicht, Entfernung zur Psychotherapiepraxis, Beschäftigungsstatus, Einkommen, finanzielle Lage, Beziehungsstatus, Kinder, Migration, Ethnizität) und Daten zu Vor-/Begleitbehandlungen (psychotherapeutische Vorbehandlung, begleitende medikamentöse Behandlung, psychische/physische Risikofaktoren) auch Daten zum Schweregrad der depressiven oder der Angst-Erkrankung erhoben. Darüber hinaus erfolgt die Erhebung von: Remission (= Nachlassen der Symptome), Response (= Ansprechen auf die Behandlung), Lebensqualität, Behandlungszufriedenheit, wahrgenommene Therapiebeziehung, Kosten-/Inanspruchnahme von Gesundheitsleistungen, Erkrankungsschweregrad und -chronizität, unerwünschte Ereignisse, negative Kindheitserfahrungen, soziale Unterstützung, Persönlichkeit, suizidales Erleben und Verhalten, Einsamkeit, Selbstwirksamkeit, Selbstmanagement, Selbstfürsorge, individuelle Therapieziele, Therapeutic agency (= Gefühl der Patient:innen, sich aktiv einbringen zu können), Übungsdurchführung, grundlegende Fertigkeiten kognitiver Verhaltenstherapie, Erwartungen/Einstellungen bezüglich der Therapie, mögliche Gründe für ein Ausscheiden aus der Studie sowie Empowerment. Die Erhebungen erfolgen zu Studieneinschluss sowie 6, 12, 18, 24 Wochen und ggf. 12 Monate sowie 24 Monate nach Studieneinschluss.

Zusätzlich werden im Rahmen von Telefon-/Videointerviews mit Patient:innen und Therapeut:innen Daten erfasst. Zu Studieneinschluss und 18 Wochen danach werden mit allen Patient:innen jeweils klinische Diagnoseinterviews (SKID, QIDS, HAM-A, SAE) per Telefon-/Videokonferenzinterviews durchgeführt. Mit ausgewählten Patient:innen und Therapeut:innen werden zudem nach Behandlungsende qualitative Telefon-/Videointerviews über die Erfahrungen mit PSYCHOnlineTHERAPIE geführt. Für qualitative Telefon-/Videointerviews erfolgt eine gesonderte Einwilligungserklärung. Therapeut:innen halten den Ein- und Ausschluss von Patient:innen fest und liefern ebenfalls Daten im Rahmen von Online-Befragungen. Seitens der Universität Ulm werden Nutzungsdaten der Online-Sitzungen sowie Mobile Sensing Daten (Smartphone-Nutzungsdaten, gesonderte Teilnahmeinformation und Einwilligungserklärung) erhoben.

Darüber hinaus werden durch die Krankenkassen (AOK Baden-Württemberg und Bosch BKK) Routinedaten in pseudonymisierter Form bereitgestellt, die weder Ihren Namen noch Ihr Geburtsdatum enthalten. Ein Rückschluss auf Ihre Person ist somit ausgeschlossen. Folgende Datenkategorien aus dem Zeitraum 01.10.2020 bis einschließlich 30.11.2023 werden von der AOK Baden-Württemberg und der Bosch BKK pseudonymisiert an die unter Abschnitt 7 aufgeführte Institution (Stelle für Gesundheitsökonomie der Friedrich-Alexander-Universität Nürnberg-Erlangen) übermittelt:

- Versichertenstammdaten
- Ambulante Leistungen
- Ambulante Diagnosen
- Ambulantes Operieren
- Arzneimittelverordnungen
- Stationäre Behandlungen
- Stationäre Prozeduren
- Stationäre Diagnosen
- Hochschulambulanzen / PIAs
- Heilmittel
- Hilfsmittel
- Ambulante Rehabilitation
- Stationäre Rehabilitation
- AU und Krankengeld
- AU Diagnose
- AU Erwerbsminderungsrente

Außerdem erhält die Stelle für Gesundheitsökonomie der FAU Ihre Daten im Rahmen der gesundheitsökonomischen Evaluation aus der Primärdatenerhebung in pseudonymisierter Form. Die pseudonymisierten Daten aus der Primärdatenerhebung werden zum Zwecke der wissenschaftlichen Begleitung mit den pseudonymisierten Daten Ihrer Krankenkasse (AOK Baden-Württemberg, Bosch BKK) bei der Stelle für Gesundheitsökonomie der FAU zusammengeführt und ausgewertet. Der Rückschluss auf Ihre Person ist ausgeschlossen. Die Studie ist durch die Ethikkommission der Deutschen Gesellschaft für Psychologie (DGPs) genehmigt worden.

5. Analyseergebnisse der Daten

Die Daten werden in pseudonymisierter Form erhoben und ausgewertet. Aus ihnen sollen Informationen zur Durchführbarkeit, (Kosten-)Effektivität, Akzeptanz, Optimierungspotenzialen, möglichen Risiken und Nebenwirkungen und beteiligten Variablen beim Einsatz strukturierter Online-Sitzungen zur Unterstützung der psychotherapeutischen Routinebehandlung bei Patient:innen mit depressiver Erkrankung und/oder Angsterkrankung erhalten werden. Weitere persönliche oder schützenswerte Daten ergeben sich aus der Analyse nicht.

6. Lagerung und Weitergabe von Daten

Die Daten der Befragungen werden mittels der Befragungssoftware LimeSurvey erhoben und auf den internen Servern der Friedrich-Alexander-Universität Erlangen-Nürnberg gespeichert. Diese befinden sich in einem gesicherten Serverraum, dessen Zugang nur über Authentifizierung für berechtigtes Personal möglich ist (getrennte Server für Webspace und Datenbank) und werden auf einem Netapp-Fileserver vorgehalten und zusätzlich von einem Backup-System mindestens 3 Monate gesichert. Der Zugriff auf den Webspace erfolgt über eine Funktionskennung, die Zugriff allein auf den eigenen Webbereich bietet. Jeder Webspace erhält ein SSL Zertifikat vom DFN. Dieses ist gemäß den DFN Richtlinien beantragt und verwaltet. Der Zugriff auf interne Keys des Zertifikats ist nur damit betrauten Personal des Regionalen Rechenzentrums Erlangen (RRZE) möglich. Die Kommunikation erfolgt über diesen verschlüsselten Kanal (AES 256).

Im Rahmen der Studie werden Daten in der Praxis/Ambulanz der Therapeut:innen auf einem Tablet erhoben. Auf diesem Tablet befindet sich eine verschlüsselte Kodierliste mit Namen und Studien-IDs der behandelten Patient:innen. Mittels einer App wird auf die Online-Befragungen über LimeSurvey weitergeleitet. Es werden keine weiteren Daten auf dem Tablet gespeichert. Das Tablet wird gemäß DSGVO unter Sorgfaltspflicht der Therapeut:innen in deren Praxis zugriffsbeschränkt aufbewahrt.

Die Online-Sitzungen werden auf der passwortgeschützten Online-Plattform (eSano) der Universität Ulm dargeboten. Die Plattform eSano wird vom Institut für Datenbanken und Informationssystem (DBIS) der Universität Ulm verwaltet. Die Plattform besteht aus einem Content Management System zur Erstellung von Inhalten, einer Patient:innen-Plattform und einer Therapeut:innen-Plattform. Über eSano werden folgende Daten des Nutzerverhaltens erhoben: Nutzung der Plattform im Hinblick auf Patient:innen-Therapeut:innen-Interaktionen (z.B. Angaben zur Anzahl und Art der Kontakte mit den jeweiligen Therapeut:innen); Nutzung der Plattform im Hinblick auf die Online-Sitzungen (z.B. Anzahl der Logins, Bearbeitungszeitraum, Abbruchrate). Alle Daten, die über die Plattform erhoben werden, werden auf den Servern der Universität Ulm verschlüsselt gespeichert.

Wenn Sie bei der AOK Baden-Württemberg oder der Bosch BKK versichert sind und der Einwilligungserklärung zustimmen, wird ein Abruf von Versichertendaten initiiert. Die Datenlieferung erfolgt für den Zeitraum von einem Quartal vor Interventionsbeginn im Rahmen des Projekts bis ein Jahr nach Interventionszeitraum im Rahmen des Projekts. Diese werden mit den Evaluationsdaten aus Ihren Onlinebefragungen verknüpft und dienen dem Zweck einer gesundheitsökonomischen Analyse in dieser Studie. Hierzu leitet das Studienteam der FAU Ihre im Rahmen der Einwilligungserklärung erhobenen Teilnahmedaten (Vorname, Nachname, Geburtsdatum, KV-Nummer) an Ihre Krankenkasse weiter. Die Krankenkassen haben jedoch keinen Zugriff auf die Zugehörigkeit zu den Studienbedingungen sowie auf Evaluationsdaten. Die Krankenkassen versichern, dass ihren Versicherten durch die Teilnahme an dieser Studie keinerlei Nachteile entstehen sowie ein Speichern und Zusammenführen mit bestehenden Informationen zu Versicherten nicht stattfinden wird.

7. Beteiligte, Datenflüsse und speichernde Stellen

Verantwortliche	Zuständigkeit	Form der vorliegenden Daten
Abteilung Klinische Psychologie und Psychotherapie (Prof. Dr. Baumeister) Institut für Psychologie und Pädagogik Universität Ulm Lise-Meitner-Straße 16 89081 Ulm	Studienleitung/ Konsortialführung, zuständig für die Studienleitung	Pseudonymisierte Daten der Online-Plattform *(Weitergabe an FAU)*, Pseudonymisierte Daten der Mobile Sensing Substudie (Weitergabe an FAU) Pseudonymisierte Daten der Evaluation *(durch FAU zur Verfügung gestellt)*
Institut für Datenbanken und Informationssysteme (Prof Dr. Reichert und Dr. Pryss) Universität Ulm James-Franck Ring 89081 Ulm	Konsortialpartner, IT-Support	Pseudonymisierte Daten der Online-Plattform und Pseudonymisierte Daten der Mobile Sensing Substudie *(Weitergabe an UULM, Abteilung Klinische Psychologie und Psychotherapie)*
Friedrich-Alexander-Universität Erlangen-Nürnberg Schlossplatz 4 91054 Erlangen <u>Ausführende Stelle:</u> Lehrstuhl für Klinische Psychologie und Psychotherapie (Prof. Dr. Matthias Berking und Assoc. Prof. Dr. David D. Ebert) Friedrich-Alexander-Universität Erlangen-Nürnberg Nägelsbachstr. 25a 91052 Erlangen 1. Evaluationsteam der FAU 2. Stelle für Gesundheitsökonomie der FAU	Konsortialpartner, Zuständigkeit für Evaluation	1. Klardaten, Pseudonymisierte Daten der Evaluation *(Weitergabe an UULM, Abteilung Klinische Psychologie und Psychotherapie)*, Pseudonymisierte Daten der Online-Plattform, *(zur Verfügung gestellt durch UULM, Abteilung Klinische Psychologie und Psychotherapie)* 2. Pseudonymisierte Routinedaten *(Weitergabe an Evaluationsteam der FAU)*, Pseudonymisierte Daten der Evaluation

AOK Baden-Württemberg Integriertes Leistungsmanagement Presselstraße 19 70191 Stuttgart	Konsortialpartner, zuständig für Vertragsklärung, Dissemination und Routinedaten	Routinedaten *(pseudonymisierte Weitergabe an Stelle für Gesundheitsökonomie der FAU)*
Bosch BKK Versorgung und Gesundheit Kruppstraße 19 70469 Stuttgart	Konsortialpartner, zuständig für Vertragsklärung, Dissemination und Routinedaten	Routinedaten *(pseudonymisierte Weitergabe an Stelle für Gesundheitsökonomie der FAU)*
MEDIVERBUND AG Vertragswesen Industriestraße 2 70565 Stuttgart	Konsortialpartner, zuständig für Rekrutierung und Abrechnung nach der Ergänzungsvereinbarung im PNP-Vertrag	Abrechnungsdaten nach der Ergänzungsvereinbarung zum PNP-Modul Psychotherapie
MEDI Baden-Württemberg e.V. Industriestraße 2 70565 Stuttgart	Kooperationspartner, zuständig für Rekrutierung und Dissemination	Keine Daten
Freie Liste der Psychotherapeuten Plochinger Straße 115 73730 Esslingen am Neckar	Kooperationspartner, zuständig für Rekrutierung und Dissemination	Keine Daten
Deutsche Psychotherapeuten Vereinigung (DPtV) Am Karlsbad 15 10785 Berlin	Kooperationspartner, zuständig für Rekrutierung und Dissemination	Keine Daten
HelloBetter – GET.ON Institut für Online-Gesundheitstrainings GmbH Oranienburger Str. 86a 10178 Berlin	Datenübertragung im Rahmen der gesundheitsökonomischen Evaluation	Pseudonymisierte Daten der Evaluation

8. Konkrete Dauer der Speicherung

Kontaktdaten sowie die Kodierliste, die der Zuordnung zu personenbezogenen Angaben dient, werden nach Abschluss der Datenerhebung (letzte:r Teilnehmer:in hat die letzte Befragung durchlaufen) gelöscht. Nach Vernichtung der Kodierliste liegen die Daten nur noch in vollständig anonymisierter Form vor und ein Rückschluss auf die einzelnen Teilnehmenden ist dann nicht mehr möglich. Diese vollständig anonymisierten Daten dürfen an Dritte zu ausschließlich wissenschaftlichen Zwecken (z.B. zu Fragestellungen, die besondere Auswertungsfähigkeiten benötigen; Zusammenführen mehrerer Datensätze für Metaanalysen; Reanalysen der Studienergebnisse durch unabhängige Forschungseinrichtungen zur Absicherung guter wissenschaftlicher Praxis) weitergegeben werden. Die Daten werden mindestens 10 Jahre nach Datenauswertung bzw. mindestens 10 Jahre nach Erscheinen einer Publikation zu dieser Studie aufbewahrt und ggf. über eine Internet-Datenbank öffentlich zugänglich gemacht.

9. Pseudonymisierungsverfahren

Die Kontaktdaten, die teilnehmende Patient:innen im Rahmen der Einwilligungserklärung angeben, werden von der Friedrich-Alexander-Universität Erlangen-Nürnberg unter dem von ihnen generierten Code (Studien-

ID) pseudonymisiert gespeichert. Ein Personenbezug ist daher nur mittels einer getrennt aufbewahrten Kodierliste möglich. Zusätzlich erfolgt die Registrierung zu den Online-Sitzungen ebenfalls über einen Code (eSano-Code), der von der Universität Ulm generiert wurde und von Therapeut:innen an ihre jeweiligen Patient:innen weitergegeben wird. Beide Codes (Studien-ID und eSano-Code) werden auf der Kodierliste von der Friedrich-Alexander-Universität Erlangen-Nürnberg gespeichert. Die Kodierliste ist nur den Studienmitarbeiter:innen der Friedrich-Alexander-Universität Erlangen-Nürnberg zugänglich und wird nach Abschluss der Datenerhebung vernichtet. Das Ende der Datenerhebung beschreibt den Zeitpunkt, zu dem der:die letzte Patient:in die letzte Befragung durchlaufen hat. Der Aufbewahrungszeitraum bis zur Vernichtung der Kodierliste ist notwendig, damit eine Kontaktaufnahme im Rahmen der Studienteilnahme möglich ist, um den teilnehmenden Patient:innen Zugang zu dem Studienangebot zu gewähren und sie zu den erforderlichen Online-Befragungen einzuladen. Nach Vernichtung der Kodierlisten liegen die Daten nur noch in vollständig anonymisierter Form vor. Ein Rückschluss auf den/die einzelne(n) Teilnehmer:in ist dann nicht mehr möglich. Ebenfalls werden von Ihrer Krankenkasse im Zuge der Bereitstellung von Abrechnungsdaten ausschließlich pseudonymisierte Daten übermittelt, die weder Ihren Namen, noch Ihre Initialen oder Ihr Geburtsdatum enthalten. Ein Rückschluss auf Ihre Person ist somit ausgeschlossen.

10. Rechtsgrundlagen

Die Rechtsgrundlage zur Verarbeitung der genannten personenbezogenen Daten bildet die Einwilligung gemäß Art. 6 (1) Buchstabe a sowie Art. 9 Abs. 2a EU-DSGVO am Ende dieses Dokumentes.

11. Widerruf seitens des Betroffenen

Sie haben das Recht, jederzeit die Einwilligung zu widerrufen (Art. 21 DSGVO). Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. (Widerruf mit Wirkung für die Zukunft, Art. 7, Abs 3 DSGVO). Richten Sie den Widerruf an:

Dr. Anna-Carlotta Zarski
Lehrstuhl für Klinische Psychologie und Psychotherapie
Friedrich-Alexander-Universität Erlangen-Nürnberg
Nägelsbachstr. 25a, D-91052 Erlangen
Tel.: +49 (0)9131 85 67570
E-Mail: evaluation@psychonlinetherapie.de

Ihnen entstehen durch den Widerruf der Teilnahme an der Studie und dem Einverständnis zur Verarbeitung der erhobenen Daten keine Nachteile. Nach Eingang des Widerrufs werden die personenbezogenen Daten anonymisiert bzw. gelöscht. Jedoch ist Ihnen eine Teilnahme an dieser besonderen Versorgungsform nicht (mehr) möglich.

12. Namen, Kontaktdaten des Verantwortlichen

Die Verantwortlichkeit für die Datenerhebung und -sicherheit im Rahmen der Studie PSYCHOnlineTHERAPIE liegt bei der Universität Ulm und der Friedrich-Alexander-Universität Erlangen-Nürnberg (geteilte Datenverantwortlichkeit). Verantwortliche für die Datenverarbeitung sind Assoc. Prof. Dr. David Daniel Ebert (Friedrich-Alexander-Universität Erlangen-Nürnberg) und Prof. Dr. Harald Baumeister (Universität Ulm). Eine Kontaktaufnahme ist über die Verantwortlichen für die Verarbeitung der personenbezogenen Daten möglich:

Dr. Anna-Carlotta Zarski
Lehrstuhl für Klinische Psychologie und Psychotherapie
Friedrich-Alexander-Universität Erlangen-Nürnberg
Nägelsbachstr. 25a, D-91052 Erlangen
Tel.: +49 (0)9131 85 67570
E-Mail: evaluation@psychonlinetherapie.de

Rückfragen zur Studienteilnahme, welche die Kenntnis über die Zuordnung von Personenangaben zu im weiteren Verlauf der Studie erhobenen Daten voraussetzen, können ausschließlich von dieser Stelle bearbeitet werden. Ebenfalls können über die angegebene Adresse Betroffenenrechte geltend gemacht werden, bspw. bei Wunsch auf Löschung der erhobenen Daten. Für allgemeine Fragen und weiterführende Informationen zur Studie besteht zudem ebenfalls die Möglichkeit der Kontaktaufnahme über diese Adresse.

13. Kontaktdaten des Datenschutzbeauftragten

Die für die Datenverarbeitung verantwortlichen Datenschutzbeauftragten an der Friedrich-Alexander-Universität Erlangen-Nürnberg und an der Universität Ulm sind zu erreichen unter folgenden Kontaktdaten:

Norbert Gärtner, RD
Datenschutzbeauftragter
Friedrich-Alexander-Universität Erlangen-Nürnberg
Schlossplatz 4
91054 Erlangen
Tel.: +49 9131 85-70830
E-Mail: norbert.gaertner@fau.de

Irina Weiß
Datenschutzbeauftragte
Universität Ulm
Helmholtzstraße 16
89081 Ulm
Tel.: +49 (7542) 949 21 09
E-Mail: dsb@uni-ulm.de

14. Hinweis auf Rechte der Betroffenen

Gemäß Art. 13 Abs.2 der Datenschutzgrundverordnung haben Sie das Recht auf

- Auskunft (Art 15 DSGVO und §34 BDSG)
- Widerspruch (Art. 21 DSGVO 2018 und §36 BDSG)
- Datenübertragbarkeit (Art 20 DSGVO)
- Löschung (Art 17 DSGVO und §35 BDSG)
- Einschränkung der Verarbeitung (Art 18 DSGVO)
- Berichtigung (Art 16 DSGVO)

Möchten Sie eines dieser Rechte in Anspruch nehmen, wenden Sie sich bitte an:

Lehrstuhl für Klinische Psychologie und Psychotherapie
Friedrich-Alexander-Universität Erlangen-Nürnberg
Nägelsbachstr. 25a, 91052 Erlangen
Tel.: +49 (0)9131 85 67570
evaluation@psychonlinetherapie.de

Weiterhin haben Sie das Recht, Beschwerde bei der Aufsichtsbehörde einzulegen:

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg
Dr. Stefan Brink
Postfach 10 92 32, 70025 Stuttgart
Telefon: +49 (0)711 6155410
E-Mail: poststelle@lfdi.bwl.de
Web: http://www.baden-wuerttemberg.datenschutz.de

Bayerische Landesbeauftragte für den Datenschutz
Herr Prof. Dr. Thomas Petri
Postfach 22 12 19
Wagmüllerstraße 18, 80538 München
Telefon: +49 (0)89 212672-0
Telefax: +49 (0)89 212672-50
E-Mail: poststelle@datenschutz-bayern.de
Homepage: https://www.datenschutz-bayern.de/

15. CHECKLISTE ZUM EINSCHLUSS IN PSYCHONLINETHERAPIE

Auszufüllen durch Ihre:n Therapeut:in

Hiermit wird bestätigt, dass folgende Einschlusskriterien vorliegen:

- ☐ Teilnehmende:r Patient:in ist mindestens 18 Jahre alt
- ☐ Teilnehmende:r Patient:in hat die Diagnose einer depressiven Störung und/oder Angststörung entsprechend der ICD-Liste des PNP-Selektivvertrags
- ☐ Teilnehmende:r Patient:in ist Versicherte:r der AOK Baden-Württemberg und nimmt am FacharztProgramm der AOK Baden-Württemberg teil bzw. schreibt sich zeitgleich mit der Einschreibung in PSYCHOnlineTHERAPIE in dieses ein, sofern die Voraussetzungen zur Sofortabrechnung (SANE) vorliegen ALTERNATIV teilnehmende:r Patient:in ist Versicherte:r der Bosch BKK und nimmt am Facharztprogramm der Bosch BKK teil bzw. schreibt sich zeitgleich mit der Einschreibung in PSYCHOnlineTHERAPIE in dieses ein, sofern die Voraussetzungen zur Sofortabrechnung (SANE) vorliegen
- ☐ Teilnehmende:r Patient:in verfügt über einen Internetzugang sowie ein internetfähiges Endgerät (PC/Laptop/Smartphone/Tablet)
- ☐ Teilnehmende:r Patient:in verfügt über ausreichende Deutschkenntnisse (Wort und Schrift)
- ☐ Teilnehmende:r Patient:in hat keine ICD-10-F2 Diagnose
- ☐ Es liegen keine klinischen Ausschlusskriterien vor, die gegen eine Teilnahme der:des Patient:in an PSYCHOnlineTHERAPIE sprechen

16. Einwilligungserklärung zur Studienteilnahme und Zur Erhebung und Verarbeitung personenbezogener Daten

Über Ziele, Inhalt, Vorgehensweise und Risiken der obengenannten Studie sowie die Befugnis zur Einsichtnahme in die erhobenen Daten bin ich schriftlich und mündlich ausreichend informiert worden. Ich hatte die Gelegenheit Fragen zu stellen und habe hierauf Antwort erhalten. Über die Folgen eines jederzeit möglichen Widerrufs der datenschutzrechtlichen Einwilligung bin ich aufgeklärt worden. Ich bin darüber informiert worden, dass durch meinen Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird. Ich kann jederzeit eine Löschung all meiner Daten verlangen. Wenn allerdings die Kodierliste bereits gelöscht ist, kann mein Datensatz nicht mehr identifiziert und also auch nicht mehr gelöscht werden. Meine Daten sind dann anonymisiert. Ich bin einverstanden, dass meine vollständig anonymisierten Daten zu Forschungszwecken weiterverwendet werden können. Dazu werden sie mindestens 10 Jahre nach Datenauswertung, bzw. mindestens 10 Jahre nach Erscheinen einer Publikation zu dieser Studie aufbewahrt.

Ich hatte ausreichend Zeit, mich für oder gegen die Teilnahme an der Studie zu entscheiden. Eine Kopie der Teilnahmeinformation und Einwilligungserklärung mit meinen persönlichen Angaben erhalte ich im Anschluss per E-Mail an die von mir angegebene E-Mail-Adresse.

Einwilligung zur Studienteilnahme

☐ Hiermit willige ich freiwillig in die Teilnahme an der Studie „PSYCHOnlineTHERAPIE" ein.

Einwilligung zur Datenverarbeitung

☐ Hiermit willige ich freiwillig in die oben beschriebene Erhebung und Verarbeitung meiner personenbezogenen Daten ein.

Einwilligung zur Weitergabe von Routinedaten durch Ihre Krankenkasse

Hiermit willige ich freiwillig in die oben beschriebene Weitergabe meiner pseudonymisierten Routinedaten durch meine Krankenkasse (AOK Baden-Württemberg / Bosch BKK) ein.

☐ JA ☐ NEIN

Zusatzvereinbarung für künftige Kontaktaufnahmen im Rahmen dieser Studie

Ich gebe mein Einverständnis, dass ich im Falle einer Fortführung dieser Studie oder von Anschlussstudien kontaktiert werden darf. Dafür werden meine Kontaktdaten an der Friedrich-Alexander-Universität Erlangen-Nürnberg gespeichert. Mein Einverständnis zur Aufbewahrung bzw. Speicherung dieser Daten kann ich jederzeit widerrufen, ohne dass mir daraus Nachteile entstehen. Ich kann jederzeit eine Löschung all meiner Daten verlangen.

☐ JA ☐ NEIN

_____ _____

Ort, Datum Unterschrift der einwilligenden Person

C eSano Privacy Policy

Informationen zum Datenschutz

Sehr geehrte Nutzer:innen der Plattform eSano,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Deshalb informieren wir Sie an dieser Stelle, zu welchem Zweck wir Ihre Daten erheben, speichern oder weiterleiten. Sollten Sie die Plattform im Rahmen einer Studie nutzen, können weitere datenschutzrelevante Anforderungen in den dazugehörigen Teilnahmeinformationen bzw. Einwilligungserklärungen Geltung finden. Der Information können Sie auch entnehmen, welche Rechte Ihnen bezüglich Ihrer personenbezogenen Daten zusteht.

1. Verantwortlicher für die Datenverarbeitung

Verantwortlicher für die Datenverarbeitung ist genannt gem. Art. 4 Abs. 7 Datenschutzgrundverordnung (DSGVO) die

Universität Ulm

89069 Ulm

Telefon +49 (0)731/50-10

Telefax +49 (0)731/50-22038

Die Universität Ulm ist eine Körperschaft des öffentlichen Rechts, die durch den Präsidenten Prof. Dr.-Ing. Michael Weber (praesident(at)uni-ulm.de) oder durch den Kanzler Dieter Kaufmann (kanzler(at)uni-ulm.de) vertreten wird.

Bei Fragen rund um den Datenschutz wenden Sie sich bitte an dsb(at)uni-ulm.de oder senden einen Brief mit dem Zusatz "Datenschutzbeauftragte" an die o. g. Adresse.

Weitere spezifische Informationen bezüglich der jeweiligen Studie, an der Sie teilnehmen, finden Sie in den zugehörigen Teilnahmeinformationen bzw. Einwilligungserklärungen.

2. Datenkategorien, Zweck und Rechtsgrundlage der Datenverarbeitung

eSano ist eine E-Health-Plattform zur technischen Unterstützung von Internet- und Mobile-basierten Interventionen (IMIs). IMIs können als orts- und zeitunabhängige Angebote dazu beitragen die Gesundheitsversorgung zu verbessern. Die eSano Plattform ermöglicht es, IMIs kollaborativ zu erstellen, Nutzenden, wie Patient:innen oder Personen, die eine Gesundheitsförderungsintervention in Anspruch nehmen, bereitzustellen und diese, je nach Interventionsansatz, therapeutisch zu begleiten. Die Plattform besteht aus drei Teilplattformen: einem webbasierten Content-Management-System, einer webbasierten E-Coach Plattform und einer Cross-Plattform Nutzenden-Applikation. Alle Daten, die über die Plattform erhoben werden, werden auf den in Deutschland verorteten Servern der STRATO AG gesichert gespeichert.

Es werden die folgenden personenbezogenen Daten von Ihnen verarbeitet:

- E-Mail-Adresse
- Eingaben in Interventionen und Tagebüchern
- Konversationen mit E-Coaches und anderen Nutzenden
- Nutzungsdaten der Plattform in Hinblick auf das allgemeine Nutzungsverhalten (z.B. Zeitpunkt der Logins) sowie auf das Online-Interventionsprogramm (z.B. Startzeitpunt der Bearbeitung, Abschlusszeitpunkt einer Lektion)

Wir verarbeiten personenbezogene Daten unserer Nutzer:innen grundsätzlich nur, soweit dies zur Bereitstellung einer funktionsfähigen Plattform sowie unserer Inhalte und Leistungen erforderlich ist. Die Verarbeitung personenbezogener Daten unserer Nutzer:innen erfolgt nur nach freiwilliger, informierter Einwilligung der:des Nutzerin:Nutzers. Sollten Sie diese Plattform im Rahmen einer Studie nutzen, können Sie weitere Details den jeweils zugehörigen Teilnahmeinformationen bzw. der Einwilligungserklärung entnehmen. Rechtsgrundlage für die Verarbeitung ist in diesem Fall Ihre Einwilligung zur Teilnahme an der jeweiligen Studie gem. Art. 6 Abs. 1 lit. a EU-DSGVO.

Für den Fall, dass lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person eine Verarbeitung personenbezogener Daten erforderlich machen, dient Art. 6 Abs. 1 lit. d DSGVO als Rechtsgrundlage.

Weiterhin werden Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO verarbeitet, die als Teil einer Studie erfasst werden. Gesundheitsdaten umfassen dabei alle Daten, die Aufschluss über die körperliche oder geistige Verfassung geben und sich auf eine natürliche Person beziehen.

Darunter fallen beispielsweise:

- Tagebuchdaten, die den Symptomverlauf oder persönlichen Notizen beinhalten
- Antworten in Freitextfeldern als Teil einer Intervention
- Konversationen, unter anderem mit anderen Patient:innen oder eCoaches

Gesundheitsdaten werden dabei nur durch Ihre ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a) DSGVO verarbeitet. Nur durch diese Einwilligung besteht die Möglichkeit, die eSano Plattform uneingeschränkt nutzen zu können.

Unsere Website verwendet Cookies. Das sind kleine Textdateien, die Ihr Webbrowser auf Ihrem Endgerät speichert. Cookies helfen uns dabei, unser Angebot nutzerfreundlicher, effektiver und sicherer zu machen. Einige Cookies sind "Session-Cookies." Solche Cookies werden nach Ende Ihrer Browser-Sitzung von selbst gelöscht. Hingegen bleiben andere Cookies auf Ihrem Endgerät bestehen, bis Sie diese selbst löschen. Solche Cookies helfen uns, Sie bei Rückkehr auf unserer Website wiederzuerkennen. Mit einem modernen Webbrowser können Sie das Setzen von Cookies überwachen, einschränken oder unterbinden. Viele Webbrowser lassen sich so konfigurieren, dass Cookies mit dem Schließen des Programms von selbst gelöscht werden. Die Deaktivierung von Cookies kann eine eingeschränkte Funktionalität unserer Website zur Folge haben. Das Setzen von Cookies, die zur Ausübung elektronischer Kommunikationsvorgänge oder der Bereitstellung bestimmter, von Ihnen erwünschter Funktionen (z.B. Warenkorb) notwendig sind, erfolgt auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Als Betreiber dieser Website haben wir ein berechtigtes Interesse an der Speicherung von Cookies zur technisch fehlerfreien und reibungslosen Bereitstellung unserer Dienste. Sofern die Setzung anderer Cookies (z.B. für Analyse-Funktionen) erfolgt, werden diese in dieser Datenschutzerklärung separat behandelt.

In Server-Log-Dateien erheben und speichern wir automatisch Informationen, die Ihr Browser automatisch an uns übermittelt. Dies sind:

- Besuchte Seite auf unserer Domain
- Browsertyp und Browserversion
- Verwendetes Betriebssystem
- Referrer URL
- Hostname des zugreifenden Rechners
- Datum und Uhrzeit der Serveranfrage
- IP-Adresse

Es findet keine Zusammenführung dieser Daten mit anderen Datenquellen statt. Grundlage der Datenverarbeitung bildet Art. 6 Abs. 1 lit. b EU-DSGVO.

3. TLS-Verschlüsselung

Aus Sicherheitsgründen und zum Schutz der Übertragung vertraulicher Inhalte, die Sie an uns als Seitenbetreiber senden, nutzt unsere Website eine SSL-bzw. TLS-Verschlüsselung. Damit sind Daten, die Sie über diese Plattform übermitteln, für Dritte nicht mitlesbar. Sie erkennen eine verschlüsselte Verbindung an der „https://" Adresszeile Ihres Browsers und am Schloss-Symbol in der Browserzeile.

4. Speicherung Ihrer Daten

Die personenbezogenen Daten der betroffenen Person werden gelöscht oder der Personenbezug entfernt, sobald der Zweck der Speicherung, wie die ordnungsgemäße Funktionalität der Plattform oder die Auswertung zu Forschungszwecken, entfällt und sofern einer Löschung keine sonstigen berechtigten Interessen des für die Verarbeitung Verantwortlichen entgegenstehen. Bitte beachten Sie, dass sich hinsichtlich der Löschfrist bei Teilnahme an einer Studie oder einem Forschungsprojekt, mit Bezug zu eSano Abweichungen ergeben können. Bitte informieren Sie sich hierzu bei dem jeweiligen Studien-/Forschungsleiter.

5. Empfänger Ihrer Daten

Im Rahmen der Nutzung der Online-Plattform werden Ihre Daten, sofern in den Teilnahmeinformationen bzw. der Einwilligungserklärung der jeweiligen Studie, an der Sie ggf. teilnehmen, nicht anders benannt, von der Abteilung für Klinische Psychologie und Psychotherapie der Universität Ulm zu wissenschaftlichen Zwecken verwendet.

6. Datenverarbeitung durch einen Dritten

Für das Hosting der Online-Plattform nutzen wir einen Server der Firma

STRATO AG

Pascalstraße 10

10587 Berlin

Ihre eingegebenen Daten werden für uns bei der Firma STRATO AG verarbeitet. Alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen, um Ihre personenbezogenen Daten vor Verlust und Missbrauch zu schützen, werden von uns und in unserem Auftrag von der Firma STRATO AG getroffen.

7. Widerruf Ihrer Einwilligung zur Datenverarbeitung

Die Einwilligung zur Datenverarbeitung ist freiwillig. Sie haben das Recht, Ihre Einwilligung jederzeit und ohne Angaben von Gründen zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Sollten Sie die Plattform im Rahmen einer Studie nutzen, richten Sie Ihren Widerruf als formlose Mitteilung an die in Teilnahmeinformationen bzw. der Einwilligungserklärung Ihrer jeweiligen Studie genannte Adresse.

8. Ihre Rechte als Betroffener

Zum Schutz Ihrer personenbezogenen Daten stehen Ihnen folgende Rechte zu:

- Ihre Einwilligung widerrufen (Art. 7 Abs. 3 DSGVO)
- Auskunft über die Sie betreffenden personenbezogenen Daten zu erhalten (Art. 15 DSGVO),
- unrichtige Daten berichtigen zu lassen (Art. 16 DSGVO),
- unter bestimmten Voraussetzungen die Löschung oder Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen (Art. 17, 18 DSGVO),
- Widerspruch gegen die Verarbeitung Ihrer Daten einzulegen (Art. 21 DSGVO),
- Ihre Daten zu erhalten und an andere von Ihnen bestimmte Stellen übertragen (Art. 20 DSGVO).
- eine Beschwerde einreichen (Art. 77 DSGVO)

Sie haben das Recht, sich an die zuständige Aufsichtsbehörde für den Datenschutz zu wenden, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Die für uns zuständige Aufsichtsbehörde ist der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg.

Weitere Informationen und Ansprechpartner:innen hierzu finden Sie in den Teilnahmeinformationen bzw. der Einwilligungserklärung der jeweiligen Studie, an der Sie teilnehmen..

D eSano On- and Offboarding

Einarbeiten neuer Projektmitglieder

1. Belehrung zur Relevanz von Datenschutz
2. Einführung in "Secure Coding" Praktiken
3. Verweis auf Uni Stelle zum Ausleihen von Hardware (ios, Android)
4. Berechtigungen werden für Dev-Tools (Gitlab, Mattermost) erteilt. AuthN über Uni LDAP, AuthZ im jeweiligen Tool nach Least-Privilege

Relevante Systeme:

- AAS2 Systeme: Accounts im Backend
- Dev System: Gitlab, Mattermost
- Div: lokale Accounts (SSH, FTP, ...)

Projektende

1. Berechtigungen für Zugänge entziehen
2. Sicherstellen, dass alle ausgeliehene Hardware zurückgegeben wurde
3. Aktuell erteilte Berechtigungen überprüfen (auf lokale Konten oä)

Relevante Systeme:

- AAS2 Systeme: Accounts im Backend
- Dev System: Gitlab, Mattermost
- Div: lokale Accounts (SSH, FTP, ...)

E Secure Coding

1. Top 10 Web Application Security Risks

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

OWASP Top Ten

2. OWASP Secure Coding Practices

This technology agnostic document defines a set of general software security coding practices, in a checklist format, that can be integrated into the software development lifecycle. Implementation of these practices will mitigate most common software vulnerabilities.

- Input Validation
- Output Encoding
- Authentication and Password Management
- Session Management
- Access Control
- Cryptographic Practices
- Error Handling and Logging
- Data Protection
- Communication Security
- System Configuration
- Database Security
- File Management
- Memory Management
- General Coding Practices

OWASP Secure Coding Practices-Quick Reference Guide

3. NPM - Best Practices

The Snyk security best practice contains security tips for NPM related code.

https://snyk.io/blog/ten-npm-security-best-practices/

4. Secure Coding Training

The following sites offer training to fix coding vulnerabilities in a controlled environment. It reiterates the important subjects of the OWASP Secure Coding Practices.

fix vulnerabilities

- codebashing
- secure code warrior

exploit vulnerabilities

- WebGoat
- BodgeIt
- Altoro mutual

F Risk Assessment

Risikoabschätzung eSano

Datenintegrität

Risiko:	Datenverlust
Ursache:	Abbruch der Internetverbindung
Vermeidung/Verminderung:	Automatisches Zwischenspeichern je Seite der Lektion bzw. alles auf dem Gerät zwischengespeichert
Kommentare:	
Schweregrad	Gering (1) -> Gering (1)
Häufigkeit	Gelegentlich (3) -> Theoretisch möglich (1)

Risiko:	Datenverlust
Ursache:	Schließen des Browsers oder Browserfensters bzw. Klicken auf anderen Button (insbes. Schaltfläche auf der linken Seite) oder Browser-Zurück-Button (?) – vor allem statt „Abschicken" (oder wenn Abschicken noch lädt)
Vermeidung/Verminderung:	Automatisches Zwischenspeichern je Seite der Lektion und Warnmeldung bevor die Seite verlassen wird
Kommentare:	
Schweregrad	Gering (1) -> Gering (1)
Häufigkeit	Gelegentlich (3) -> Selten (2)

Risiko:	Datenschutzproblem
Ursache:	Speichern des Passworts auf nicht-persönlichem Computer
Vermeidung/Verminderung:	Warnmeldung vor Speichern des Passworts (? – bzw. im Text beim Einloggen)
Kommentare:	
Schweregrad	Kritisch (2) -> Kritisch (2)
Häufigkeit	Selten (2) -> Theoretisch möglich (1)

Produktfunktionalität

Risiko:	Keine Benutzung mehr möglich
Ursache:	Passwort vergessen
Vermeidung/Verminderung:	Funktion Passwort wiederherstellen auf Startseite
Kommentare:	
Schweregrad	Gering (1) -> Gering (1)
Häufigkeit	Gelegentlich (3) -> Theoretisch möglich (1)

Risiko:	Benutzung wird unattraktiv, Patient:in unzufrieden
Ursache:	Keine neuen Lektionen vom eCoach freigeschaltet
Vermeidung/Verminderung:	Möglichkeit Nachrichten an eCoach zu senden bzw. „Neue Lektion freischalten" als Task/Reminder
Kommentare:	

Schweregrad	Kritisch (2) -> Kritisch (2)
Häufigkeit	Gelegentlich (3) -> Selten (2)

Risiko:	Benutzung wird unattraktiv, Patient:in unzufrieden
Ursache:	Nachrichten werden vom eCoach nicht beantwortet
Vermeidung/Verminderung:	Reminder bei unbeantworteten Nachrichten an eCoach (ggf. für Blended Ansätze auch Möglichkeit Reminder abzuschalten bzw. „Habe schon geantwortet“ zu klicken), eCoach kann bei Nicht-Ausführung der Aufgaben gelöscht werden (eCoach-Manager)
Kommentare:	

Risiko:	Benutzung wird unattraktiv, eCoach unzufrieden bzw. nutzlose Arbeitsbelastung
Ursache:	Patient:in führt Intervention nicht ordnungsgemäß durch, wird ausfällig, schickt oder antwortet unpassende Texte
Vermeidung/Verminderung:	Melden-Funktion (Mediator: eCoach-Manager, der Zugriff auf Antworten der Patient:innen und Nachrichtenverlauf hat (?)), eCoach kann Patient:innen löschen bzw. aus Studie ausschließen
Kommentare:	Alternativ auch Studienhotline/-mail, Ansprechpartner

Risiko:	Benutzung wird unattraktiv, Patient:in unzufrieden bzw. sogar negative gefährdende Auswirkungen (personenbezogen)
Ursache:	eCoach wird ausfällig, schickt oder antwortet unpassende Texte
Vermeidung/Verminderung:	Melden-Funktion (Mediator: eCoach-Manager, der Zugriff auf und Nachrichtenverlauf hat (?)), eCoach-Manager kann eCoach löschen bzw. aus Studie ausschließen und Patient:innen neuem eCoach zuweisen
Kommentare:	Alternativ auch Studienhotline/-mail, Ansprechpartner

Risiko:	Benutzung wird unmöglich, Patient:in unzufrieden bzw. sogar negative gefährdende Auswirkungen (personenbezogen)
Ursache:	Patient:in findet sich auf Plattform nicht zurecht
Vermeidung/Verminderung:	„Tour“ am Anfang, Intromodul mit Erklärungen (auf das man beim ersten Einloggen geleitet wird)
Kommentare:	Alternativ auch technischer Support

Personenbezogen

Risiko:	Selbstverletzendes Verhalten, ggf. Suizid
Ursache:	Suizidgedanken/-androhung per Nachricht an den eCoach und wird nicht gelesen/reagiert
Vermeidung/Verminderung:	Kontaktmöglichkeiten einschränkbar (z.B.

	PSYCHOnlineTHERAPIE), Angabe von Soforthilfenummern (Krisenhotline)
Kommentare:	

Risiko:	Selbstverletzendes Verhalten, ggf. Suizid
Ursache:	Suizidgedanken/-androhung auf Fragen in der Lektion und wird nicht gelesen/reagiert
Vermeidung/Verminderung:	eCoaches müssen bei Lektionen, bei denen Feedback notwendig ist, dieses innerhalb bestimmter Zeit abgeben, Angabe von Soforthilfenummern (Krisenhotline, ggf. auch am Ende der Lektion)
Kommentare:	

Risiko:	Selbstverletzendes Verhalten, ggf. Suizid
Ursache:	Suizidgedanken/-androhung wollen geteilt werden
Vermeidung/Verminderung:	Krisennummern auf Seite bzw. bei Blended Ansätzen Hinweis, dass Therapeut:innen kontaktiert werden können (innerhalb der Lektion zum Beispiel)
Kommentare:	

Risiko:	Keine Hilfe durch Online-Lektionen
Ursache:	Online-Lektionen werden nicht aufgerufen
Vermeidung/Verminderung:	Reminder bei noch offenen Interventionen
Kommentare:	

List of Tables

3.1 Comparison of personal data in the DPD and GDPR based on [9] and [46] 36
3.2 Best-practices with regard to Art. 5 of the GDPR based on [60] . 48

List of Figures

2.1 History of Directives and Regulations based on [2] and [10] . . . 8
2.2 Europe and the scope of the GDPR from [15] 10
2.3 EU vs. US based on [18], [19] and [20] 12
2.4 Interdependencies between eHealth and its domains based on [27], [28] and [25] 16
2.5 Federal and state laws in Germany in the context of health based on [34] 19
2.6 Relationship between standards for medical devices based on [35] and [19] 20
2.7 eSano's entities and their interactions based on [4] 22

3.1 Use case diagram of stakeholders in the GDPR based on [37] and [38] 25
3.2 PDCA cycle in the context of GDPR based on [9] and [39] 29
3.3 Difference between pseudonymization and anonymization based on [42] 31
3.4 DPIA procedure in the context of Art. 35 of the GDPR based on [44] 33
3.5 Risk classification based on [50] 40
3.6 Guidance for medical device software to comply with ISO 13485 based on [51] 41
3.7 Responsibilities of the person in charge of compliance in the context of the MDR based on [52] and [48] 43
3.8 Summary of requirements depending on role of the actor based on [58] 45
3.9 Contents of a privacy policy based on [9] and [62] 50

4.1 Decision tree to comply with the most relevant aspects of the GDPR based on [9] 55
4.2 "Data security" requirements for eHealth applications based on [69] 57
4.3 Obligations of the data processor based on [70], [9] and [47] . . 59
4.4 Information obligations and data subject rights based on [70], [9] and [47] 60
4.5 Legal bases for processing based on [70], [9] and [47] 61
4.6 eSano (patient) account deletion process from [71] 63
4.7 Excerpt of functional requirements from the eSano platform and its internal Software Requirements Specification 64
4.8 Applied decision tree based on [70], [9] and [47] 66

4.9 “eSano” Privacy Policy Part I based on Appendix C, [71] and [9] 67
4.10 “eSano” Privacy Policy Part II based on Appendix C, [71] and [9] 68
4.11 “eSano” Privacy Policy Part III based on Appendix C [71] and [9] 69
4.12 Data Integrity risk assessment based on Appendix F and [44] . . 72
4.13 Product functionality risk assessment based on Appendix F and [44] 73
4.14 Individual-related risk assessment based on Appendix F and [44] 74
4.15 Obligations of the data processor based on [70], [9] and [47] applied on eSano 76
4.16 Information obligations and data subject rights based on [70], [9] and [47] applied on eSano 77
4.17 Legal bases for processing based on [70], [9] and [47] applied on eSano 78

5.1 GDPR imposing a high burden on companies based on [76] . . 83
5.2 Articles referenced in enforcement cases from [77]. The usage of this chart has been approved from the original author 84
5.3 Clustering of 277 sanctions since March 31, 2020 from [72] . . . 85

Name: Mahatir Muhammad Said Matriculation number: 946684

Declaration

I hereby declare that I have prepared this thesis independently and without outside help. Text passages, which are based literally or in the sense of publications or lectures of other authors, are marked as such. The work has not yet been submitted to any other examination authority and has not yet been published.

Ulm, June 25, 2022 Mahatir Said

Mahatir Muhammad Said