SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informations Systems

Exploring the Legal Perspective on the Use of Privacy-Enhancing Technologies for Data Privacy Compliance

Hannah Kiel

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Informations Systems

Exploring the Legal Perspective on the Use of Privacy-Enhancing Technologies for Data Privacy Compliance

Untersuchung der rechtlichen Perspektive des Einsatzes von Privacy-Enhancing Technologies für die Einhaltung des Datenschutzes

Author:	Hannah Kiel
Supervisor:	Prof. Dr. Florian Matthes
Advisor:	Oleksandra Klymenko, M.Sc.
Submission Date:	15.09.2023

I confirm that this bachelor's thesis in informations systems is my own work and I have documented all sources and material used.

Munich, 15.09.2023 Hannah Kiel

Acknowledgments

I would like to thank my family and friends, without whom this work and this entire study would not have been imaginable. Thank you for always being by my side and for letting me rely on you.

Abstract

Modern data protection regulations, such as the General Data Protection Regulation, require the implementation of technical measures for data protection compliance. As a result, the use of technical privacy solutions has increased and will continue to do so. Privacy-Enhancing Technologies can function as technical measures to protect the rights and freedoms of individuals. Hence, research and development in these technologies has increased. Privacy-Enhancing Technologies minimize the data usage and maximize data security, but these technologies are still complex in nature and remain highly academic.

The role of legal professionals is essential in meeting the relevant legal requirements when Privacy-Enhancing Technologies are used for data privacy compliance. However, this complexity brings new problems for the legal sector. The aim of this thesis is to explore the legal perspective on the use of Privacy-Enhancing Technologies in the process of data privacy compliance. Therefore, the role of legal professionals in the process of data privacy compliance is analyzed. This will function as foundation, to explore the challenges and obstacles that legal professionals face when Privacy-Enhancing Technologies are used. Subsequently, these findings will be used to develop according solution strategies. In this context the legal applicability of Privacy-Enhancing Technologies will be investigated.

Contents

1. Introduction

As the world becomes increasingly digital, concerns about privacy are growing. According to a poll commissioned by Amnesty International, 73% of people want to see more regulation of large tech companies. In addition, 71% expressed concern about how these tech giants collect and use their personal information [1]. Large tech companies such as Amazon, Google, Meta, or Microsoft have often been criticized for questionable practices [2]. Google just paid 392 million USD to several US states [3]. The company deceived its users by tracking their location even after they turned off the feature in their settings. Google still collected sensitive information [4]. Another high-profile example is the Cambridge Analytica scandal. In 2018, Facebook harvested the data of tens of millions of its users without their permission. Cambridge Analytica obtained the data and influenced voters in political campaigns, including the 2016 U.S. presidential election and the Brexit referendum [5]. Many big tech companies make most of their profits by selling their users' data. Google makes 80% of its revenue from advertising [3]. As a result, these companies have a strong interest in maximizing the use of the data they collect. This increases the need for regulations and laws to control companies in order to protect the freedom of individuals. This has led to the rise of many data protection regulations around the world, with the GDPR at the forefront [6]. It has been described as the "toughest privacy and security law in the world" [7]. It was passed in 2016, and organizations have had to comply with it since 2018. Any organization that violates it will be fined up to 4% of its total revenue. So far, according to the GDPR Enforcement Tracker, about 4 billion in fines have been issued [8]. So there is not only a need to protect our privacy in the digital age. There are also economic benefits to complying with privacy laws and regulations.

Modern data regulations require technical measures to secure data usage [7]. New solutions, such as Privacy-Enhancing Technologies, have been developed in recent years. These technologies can maximize data security and minimize data usage [9]. This can help meet regulatory requirements. However, this increased complexity of privacy regulations creates new challenges for the legal sector. Law and technology have very different dynamics, and privacy regulation requires that these different areas be combined to ensure that our privacy is adequately protected [10]. This creates new problems for legal experts who must guide organizations through this complex legal landscape. This thesis examines the role of legal experts in the data privacy compliance process when Privacy-Enhancing Technologies are used. It seeks to identify the roles and responsibilities of legal professionals and where they can support the use of Privacy-Enhancing Technologies. It examines the challenges and obstacles they face in this process. Subsequently, according solution strategies are developed.

2. Foundations

2.1. Privacy and Technology

In this digital age, the need to protect our privacy is enormous [11]. Therefore, it is important to first define what exactly is to be protected when we speak of this concept. Warren and Brandeis were among the first to define privacy; in their essay "Right to Privacy," they refer to the "right to be left alone" in the context of privacy [12]. In addition, they state, "Our aim is to consider whether existing law provides a principle that can be invoked to protect individual privacy and, if so, what the nature and scope of that protection is" [12]. They move from the "right to be left alone" to the laws and regulations that are designed to protect that right and whether they are able to do so [12].

In the last decade, privacy law has evolved very rapidly due to technological developments [10]. Its foundation is the protection of personal information. To protect our freedom in the digital age, the principle of Privacy by Design has been enshrined in laws and regulations [11].

Privacy by Design

"Regulatory frameworks alone are not sufficient to track the evolution of the concept of privacy" [11]. As Lessig notes, whether we like it or not, "code is law", and software developers are increasingly becoming "legislators" [13]. Anna Cavoukian introduced the concept of Privacy by Design in 2009 [14]. It provides a methodology for combining privacy policies and technology. This includes not only technical design decisions and the selection of appropriate Privacy-Enhancing Technologies but also the design of business and management processes [14]. "An integrated approach is needed" to address the privacy requirements [11]. PETs could both enable and carry that trust [11].

2.2. General Data Protection Regulation

The General Data Protection Regulation, also known as GDPR, is known as the "toughest privacy and security law in the world" [15]. It is designed to protect the personal information of residents of the European Union. They are referred to as "data subjects" [7].

2.2.1. History

Europe has always been at the forefront of data protection. It has long recognized privacy as a human right [16]. "In Europe, data protection is increasingly seen as separate from right to privacy. [17]" In European law, the protection of the privacy of information is referred to as "data protection". Some countries had already enacted national data protection laws in the late 1970s and 1980s [17]. In 1990, the European Commission became concerned that national data protection laws were hampering the EU's single market. That year, it published a proposal for a Data Protection Directive. Five years later, the 1995 European Union Data Protection Directive was adopted. It aimed to harmonize member states' data protection laws and set standards for the processing and transfer of data [17]. However, with the rapid development of new technologies, it became clear that a more robust and modern framework was needed. This led to the introduction of the General Data Protection Regulation [17].

2.2.2. Fundamentals of Data Protection by Design and Default

The concept of Privacy by Design was originally proposed by the Privacy Commissioner of Ontario, Canada, Ann Cavoukian, in the 1990s [18]. She proposed seven key principles for building privacy by design [14]. Privacy by Design and Default requires data controllers to implement both technical and organizational measures to protect the rights of data subjects [7]. Articles 5, 25, and 32 of the GDPR concretize Privacy by Design [7]:

Article 25 - Data Protection by Design and Default

Article 25 is a cornerstone of data protection legislation [18]. It emphasizes the need to protect personal data from the beginning of a design phase for a new product [18]:

- Controllers are entrusted with the selection of appropriate technical measures, overseeing data processing activities to ensure their robustness
- The selection of technical measures is influenced by the state-of-the-art technology, cost implications, nature of processing, and risk likelihood
- They should be integrated at the onset and maintained throughout the data processing stage
- These measures should be proactive and demonstrably capable of mitigating potential data risks
- Technical measures that are designed to implement data protection principles

Article 5 - Data Protection Principles

Every processing activity must adhere to data protection principles. Article 5 introduces these principles. Technical measures are evaluated and benchmarked against these principles [7]:

- Lawfulness, Transparency, and Fairness: Ensuring data processing is lawful, transparent, and fair
- Purpose Limitation: Processing data only for the specific, explicit purpose for which it was collected
- Data Minimization: Ensuring only necessary data is processed. Technical measures might include data masking or automated data pruning
- Accuracy: Keeping data accurate and up-to-date
- Integrity and Confidentiality: This principle mandates protection against unauthorized or unlawful processing and accidental loss, destruction, or damage
- Accountability: Demonstrating compliance with GDPR

Article 32 - Security of Processing:

Article 32 of the GDPR also mandates appropriate technical and organizational measures to secure personal data [7]:

- Technical measures like pseudonymization and encryption should be implemented
- Technical measures should ensure confidentiality, integrity
- Availability: Personal data should be accessible and usable upon request by an authorized party without undue delay
- Resilience: The ability of systems and services processing personal data to rapidly recover and continue functioning after adverse events, such as technical failures or cyberattacks

2.3. Data Privacy Compliance

Responsible parties, also known as data controllers, are primarily responsible for complying with data protection laws [19]. An individual or group who decides how and why personal data is handled is called a controller. Someone who handles that data on their behalf, without their direct supervision, is called processor. Thus, organizations in these roles are central to privacy protection and often become the primary subjects of privacy regulation

[19]. Responsible parties as organizations must ensure that they comply with relevant laws, regulations, and standards [20].

The mandate of Privacy by Design has to be met by organizations to remain compliant with data protection regulations [7]. Therefore, technical measures have to be considered and integrated at the design stage of a product [21]. Privacy-Enhancing Technologies can serve as technical measures. They can help to fulfill the Privacy by Design mandate and thus help an organization to achieve data privacy compliance [21].

2.4. Privacy-Enhancing Technologies

Privacy-Enhancing Technologies minimize data usage and maximize data security [21]. A short overview of six Privacy-Enhancing Technologies is presented according to a report from the Information Comissioner´s Office [9]:

Homomorphic Encryption

Homomorphic encryption helps to perform computations on encrypted data. This data has not been decrypted before. This ensures that the data remains private and protected throughout the whole data life cycle [9].

Synthetic Data

Synthetic data is artificially generated data. They are generated by a data synthesis algorithm that "replicates patterns and statistical properties of real data" [21]. A model is used to generate the data [21].

Differential Privacy

Differential Privacy adds a randomized injection of noise to data. It provides a mathematical guarantee about people's indistinguishability. "Epsilon" also called privacy budget, determines the level of added noise [21].

Zero-knowledge proofs

Zero-knowledge proofs is a protocol that allows one party to prove to another party that they possess certain information without revealing the information itself [21].

Secure-multiparty computation

Secure multi-party computation allows multiple parties to jointly perform a computation on their combined information. No party has to share all of its information with each of the other parties. Each party learns only the result and not the input data of the other parties [21].

Federated Learning

In federated learning, AI models can be trained on distributed datasets. The raw data does not need to be shared. The different parties combine some of the patterns that these models have recognized into a single central model, the global model. Only the model updates are centralized and federated [9].

3. Related Work

3.1. Technology and Law

Data protection law has become increasingly important due to the rapid technological developments in the recent years. As technology evolves, the legal landscape often struggles to keep up with these rapid developments [22]. The technical-legal gap is a topic that often appears in the literature. There are several papers that address the problems and possible solutions. The Systematic Literature Review identified several papers that address these issues.

A related paper [23] addresses the challenges and obstacles that legal and technical practitioners face when technical measures are used in the process of data privacy compliance. The author identifies a variety of factors involving roles, processes, decisions, and culture surrounding the process of privacy compliance. The author presents 33 challenges faced in the implementation of technical measures. In this thesis, the focus is on the legal perspective of the implementation of Privacy-Enhancing Technologies. The emphasis will be on the solution strategies that could be implemented in order to address these challenges.

Privacy in the digital age is a recurring theme. The authors [11] explore the issue of privacy in the technological age. They provide an overview of the privacy landscape and discuss its complexities. They also evaluate the concept of Privacy By Design. They address the challenges that arise when technical and legal experts must implement this concept. The authors of [24] discuss the applicability of PETs for the Internet of Things. They provide an overview of PETs in the IoT and how they can help meet regulatory requirements and protect against potential threats.

In [10], the complexities of merging legal and technical perspectives on privacy are explored. The study highlights the challenge of communication between legal and technical experts.

There were papers that addressed the formal approaches to privacy from a legal and technical perspective. The [25] discusses how these views differ. It discusses the technical concepts of privacy and how they can be integrated into the legal framework. It focuses on Differential Privacy and how it can be aligned with legal requirements. It suggests that a fusion of privacy and technical concepts can lead to robust privacy protection. In [26] it is again examined how Differential Privacy can be implemented to meet legal requirements. Another article [27] deals with Differential Privacy in the context of the GDPR. It analyzes the compatibility of Differential Privacy with the anonymization requirements of the GDPR.

The [28] discusses how legal texts can be incorporated into requirements engineering and system development. It serves as a resource to assist requirements engineers and auditors in designing systems that comply with legal requirements. There have also been other papers dealing with achieving data privacy compliance in a technical context. The author of [29] draws parallels between legal requirements and software engineering. They propose a logical approach to verifying legal compliance using tools such as Alloy, a specification language for expressing structural constraints. The authors in [30] focus on the limitations of current legal compliance tools. The authors in [31] explore the challenges of GDPR compliance. They describe the DEFEND EU project, which is a platform to streamline GDPR compliance. They take into account different requirements and stakeholders.

In [32], the collaboration between legal and technical experts was discussed. The paper emphasizes the importance of collaboration between legal experts and software engineers in information systems. A structured process is proposed to combine their expertise.

3.2. Guidelines for Technical Measures

The following guidelines for technical and security measures help to bridge the gap between technical and legal requirements.

The Standard Data Protection Model [33] translates the GDPR's legal requirements for the technical design of a new processing activity into technical measures. It defines the key protection objectives, such as data minimization or confidentiality, and translates them into a reference catalog of required technical and organizational measures. This enables a direct translation of the legal standards of the GDPR into practicable technical implementation. It provides a common language for the dialog between legal experts and IT professionals and ensures that data protection requirements are implemented both technically and organizationally.

The "IT-Grundschutz-Kompendium" [34] from the german Federal Office for Information Security offers a comprehensive catalog of IT security measures. It focuses on the integrity and confidentiality of personal data. The guide provides organizations with a structured approach to understanding and implementing IT security measures that take privacy into account.

3.3. Guidelines for PETs

A number of guides from respected institutions have published guidance on Privacy-Enhancing Technologies in the recent months.

The Information Commissioner's Office (ICO) has published a guide on Privacy-Enhancing Technologies [21]. The guide is divided into two parts. The first provides a deeper insight

into the legal applicability of PETs in practice. The second part briefly introduces eight types of PETs and explains their risks and benefits.

The United Nations (UN) is working on the specific application of PETs for official statistics [35]. In their guide they address the specific application of Privacy-Enhancing Technologies for official statistics. It discusses the challenges and risks of using PETs in a legal context, as well as the opportunities.

The Organization for Economic Cooperation and Development (OECD) has published a guide on PETs [36]. The report examines recent technological advances and assesses the effectiveness of various PETs, highlighting both their challenges and potential benefits. It also provides an overview of current regulatory strategies and policies related to PETs. This insight is intended to help privacy regulators and policymakers understand how PETs can help with data governance.

The Royal Society has published a report on Privacy-Enhancing Technologies for data governance and collaborative analysis [22]. It outlines the current PET landscape. It looks at how PETs can enable new, innovative uses of data.

4. Methodology

4.1. Research Questions

The goal of this thesis is to explore the legal perspective on the use of Privacy-Enhancing Technologies in the process of data privacy compliance. Three research questions were defined:

- What is the role of legal experts in supporting the use of Privacy-Enhancing Technologies in the process of data privacy compliance?
- What challenges and obstacles do legal experts face in the process of data privacy compliance when Privacy-Enhancing Technologies are used?
- What solution strategies could be implemented to enhance the ability of legal experts to support the usage of Privacy-Enhancing Technologies in the process of data privacy compliance?

The first question serves as the foundation for this work. It is necessary to understand the role of legal experts in the process of data privacy compliance when Privacy-Enhancing Technologies are used, to identify challenges that can arise in this process.

Based on these findings, this thesis aims to explore the common challenges and obstacles that exist for legal professionals in this process. These challenges will be identified, clustered, and analyzed.

Finally, the third question addresses the identified challenges and proposes solution strategies that could be implemented to assist legal professionals in their assessment of Privacy-Enhancing Technologies. Finally, future work will attempt to address the starting points for implementing specific solution strategies.

4.2. Systematic Literature Review

The research is based on the three defined research questions. The goal is to gain insights into the legal perspective on Privacy-Enhancing Technologies, specifically the operational legal role in the data privacy compliance process with PETs. These insights will serve as the basis for the qualitative analysis. A systematic literature review based on the guidelines below proposed by Kitchenham [37] is conducted:

Search Strategy

The search for primary studies involves the following steps:

- Identification of synonyms in the research question
- Use of Boolean OR to link alternative words and synonyms
- Use of Boolean to link primary terms

The search terms used are as follows (i) lawyers (ii) law (iii) law (iv) privacy technologies (v) Privacy-Enhancing Technologies (vi) technology (vii) data privacy compliance. These search terms resulted in the following queries:

- Query 1: ("lawyers" OR "law" OR "legal") and ("Privacy-Enhancing Technologies" OR PET) AND ("privacy compliance")
- Query 2: "data privacy compliance"
- Query 3: ("technology" OR "IT" or "Privacy-Enhancing Technologies") AND ("law" OR "lawyers" OR "privacy compliance")

The following databases are selected for the search:

- ACM Digital Library
- Google Scholar
- IEEEXplore
- Science Direct

The first query aims to find insights into the legal perspective on Privacy-Enhancing Technologies. The second query explores the process of data privacy compliance. It is important to understand the process itself and its structure in organizations, to understand the role that legal experts play in it. The third query seeks information about the difficult interplay between technology and law. This functions as a basis to identify specific challenges that arise for legal experts in the process of data privacy compliance with Privacy-Enhancing Technologies.

Inclusion and exclusion of primary studies

Paper that meet the following inclusion criteria are included:

- They must have been published within the last 40 years
- Papers that address data privacy compliance with technical measures
- Papers that address the technical-legal collaboration

Paper that meet following exclusion criteria are excluded:

- Papers that only focus on the technical requirements of Privacy-Enhancing Technologies
- Papers that do not mention legal and regulatory aspects of Privacy-Enhancing Technologies

References

In total the author found 63 papers that are included by the criteria. In the next steps the author selected 15 papers that addressed the legal perspective on Privacy-Enhancing Technologies, data privacy compliance and the interplay of technology and law. A forward and backward search helped the author to find seven further papers that were included. The author identified a significant lack of literature regarding the practical role of legal experts in the process of data privacy compliance with PETs.

Query 1	**Query 2**	**Query 3**
[38], [23], [24], [39], [40], [41], [42], [27]	[19], [20], [16], [43]	[44], [32], [30], [10], [29], [11], [26], [25], [28], [45]

Table 4.1.: References

4.3. Qualitative Study: Interviews

The interviews follow a semi-structured approach. The participants are legal experts for data privacy compliance. A questionnaire will be created to address their role in the data privacy compliance process, the challenges in that process, and the strategies that can be implemented to address them.

The development of the questionnaire is at the heart of the qualitative analysis. The development of this questionnaire requires a good understanding of the research area in order to explore all relevant areas of interest. During the semi-structured interviews, the questionnaire can be adjusted over time as new insights are gained from the interviews and new areas are

identified. These further adjustments are also necessary to evaluate emerging challenges and solutions.

Once the questionnaire is developed and the scope of the survey is determined, the survey participants need to be identified. This includes contacting and scheduling interviews with them. They are then presented with the questions in advance to maximize responsiveness and insights from the interviews. The questionnaire can be found in the Appendix A. The interviews will be recorded and then transcribed. Subsequently, they will be analyzed manually.

To support this process, the following steps are defined, based on those described by Braun and Clarke in their Thematic Content Analysis [46]. First, the transcripts are read to familiarize oneself with the interviews. Then important parts of the interviews are annotated. The next step is to conceptualize the data. The transcribed data is then categorized into groups and the transcripts are segmented. This includes tagging the transcripts according to the identified groups. Then, it is validated whether the themes represent the data from the interviews. Finally, the interviews are analyzed by writing a summary of the interviews.

Participants

The field of data protection is a comparatively new one, which has grown immensely with the publication of the GDPR [43]. In order to gain a deeper understanding of this area, a multi-stage approach to contact is pursued:

- Personal contacts: This category includes individuals who could be contacted directly based on an existing relationship
- Top search results: Using platforms such as LinkedIn, terms such as "data privacy lawyer" or "cybersecurity lawyer" are entered to identify relevant profiles
- References: After the initial interviews are conducted, individuals referred in these conversations could be contacted

Out of a total of 70 individuals contacted, 20 interviews with 17 participants were conducted. With three participants a follow-up meeting was set to validate initial findings. 8 of these interviewees were personal contacts, 6 came through referrals, and 3 were found through top search results.

Once these contacts were identified, it was time to initiate the actual interview process:

- Formal email invitation
- Scheduling an appointment
- Preparing with a questionnaire

Statistics

The following section presents a table of the interview statistics. This table shows not only the position of the interviewee, but also the years of professional experience and the duration of each interview. The majority of the interviews were conducted with legal experts from Germany, and three interviews were conducted with legal experts from the USA, India and Brazil. In addition, two legal experts were regulators with legal and technical expertise. In particular, many of the interviewees were from large organizations, but law firms specializing in advising small and medium-sized businesses were also interviewed.

Count	Role	Industry Domain	Organizational Size	Experience	Duration
1	Head of Legal	Payments	Large-sized	5-10	50′
2	Legal counsel, Researcher	Law Firm, Academia	Medium-sized	1-3	30′
3	External counsel	Law Firm	Large-sized	20+	60′
4	Founder, Legal counsel	Law Firm	Large-sized	20+	40′
5	Legal counsel	Health	Large-sized	5-10	77′
6	Legal counsel	Law Firm	Large-sized	5-10	85′
7	Regulator	Supervisory authority	-	5-10	60′
8	Head of data privacy	Media Group	Large-sized	5-10	79′
9	Law student	Manufacturing	Large-sized		60′
10	DPO, Founder	Finance	Medium-sized	5-10	60′
11	Legal counsel	Manufacturing	Large-sized	5-10	60′
12	Regulator	Supervisory authority	Medium-sized	1-3	50′
13	General deputy manager	Telecommunications	Large-sized	1-3	30′
14	External counsel	Law Firm	Medium-sized	5-10	40′
15	External counsel	Law Firm	Large-sized	5-10	40′
16	Legal counsel, Researcher	Academia	-	1-3	30′
17	Legal counsel	Manufacturing	Medium-sized	5-10	45′

Table 4.2.: Statistics

5. The Role of Legal

This Chapter analyzes the role of legal experts in the data protection compliance process when Privacy-Enhancing Technologies are used. The focus of this Chapter is on the different roles and responsibilities of legal professionals in their legal assessment of PETs. This includes collaboration with other roles, proactive tasks, their role in the data privacy compliance process for a new product with PETs, and ongoing compliance monitoring. Finally, the supporting role of legal professionals in the privacy compliance process with PETs is visualized. The findings in this Chapter are based on the results of the interviews. Due to the lack of literature on the practical role of legal experts in the process of data privacy compliance, the main findings come from the interviews. In addition, a follow-up interview was conducted with two legal experts (I-8) (I-5) to validate the diagram and gain more insight into the practical role of legal experts in this process.

5.1. Introduction

With the introduction of the GDPR, the complexity of data protection law has increased [17]. As a result, the demand for legal experts in the field of data protection has increased. The historical role of the privacy officer was primarily IT-focused. This has changed in recent years. In the past, compliance was mainly about the technical implementation of data protection principles, for which IT specialists were best suited. However, with the publication of GDPR and other regulations, the legal complexity has increased. This has led to the need for legal assessment and interpretation in the context of data protection compliance:

> But now, due to the GDPR and other regulations, it has become a legal matter, so the IT staff sometimes reach their limits when it comes to the legal aspects. (I-3)

Within organizations, legal experts are often part of a specialized legal team focused on data protection compliance, sometimes they are not even located within general legal departments. In several cases, these teams report to the data protection officer to ensure a coordinated approach. For large projects or in smaller- or medium-sized organizations, external legal counsels are sometimes brought in. These law firms often specialize in data protection, cybersecurity, and IT law:

> It always depends on the company; I would say it depends on who shows up. Yeah, that's the thing, it varies extremely, of course. Everything varies extremely. (I-5)

It is important to note that the specific roles and responsibilities of data privacy compliance teams can vary widely from organization to organization. In highly regulated sectors, data protection teams may have an exceptionally high level of specialization. Conversely, small- and medium-sized organizations typically have legal departments that handle a broader range of legal issues, including data protection compliance.

5.2. Legal Tasks and Responsibilities

5.2.1. Cooperation

Functioning collaboration between legal experts and other roles is crucial for effective data protection compliance, especially when dealing with Privacy-Enhancing Technologies. This applies to both internal departments and external entities.

5.2.1.1. Internal Influencing Roles

Within an organization, there are several departments that influence the data privacy compliance process when Privacy-Enhancing Technologies are used. Legal experts must consider cross-organizational interests when evaluating the use of PETs.

General legal department

> We work relatively much with the legal department because that is also how we draft contracts, they also have basic or advanced knowledge, but no specialized knowledge in data protection. That means we are relatively strongly networked. (I-5)

Regarding Privacy-Enhancing Technologies, the legal department can help review and draft contracts with third-party providers. Therefore, they can help data protection experts with general legal knowledge. Often, the legal department also has an oversight role. One interviewee says that the legal department "*still has a say.*" (I-8) Therefore, it is important for legal experts to work well with the general legal department to benefit from their different expertise and to get advice.

Management

> So, if I leave that out, I have a little bit higher risk, but what is the risk? That is ultimately the decision that from my point of view, the responsible person must make. And as data protection officers, we can't say that's not possible; instead, the so-called business judgment rule applies. That is, the company must decide how much risk is acceptable. (I-3)

Management plays a crucial role in the data privacy compliance process. Management "*is a kind of direction-giver who, in the final analysis, is also responsible for data protection.*" (I-8) If there are conflicts between the different roles, management has the authority to decide where the organization will go. It must find the best compromise. They also must decide what level of risk they are willing to accept when Privacy-Enhancing Technologies are used to ensure data privacy compliance. In the end, many interviewees mentioned that the final decision must be made by the management.

Specific departments

> Most of the time you have a department where the problem comes from. (I-8)

For simplicity, we assume in this thesis that the new project is created and developed in the IT department. However, in larger organizations, there are usually various departments from which the problem and the new project can originate. It is often the case that the technical and legal department is called by the specific department:

> That in the end affects the specific department, they are leading. They are the ones who ultimately approach the individual supporting functions and say, I need this or that. (I-5)

5.2.1.2. External Influencing Roles

The usage of Privacy-Enhancing Technologies is also very much influenced by external parties, including lawmakers, regulators, and PET vendors.

Lawmakers

> And, of course, it is the legislator who ultimately sets the framework conditions. (I-5)

Lawmakers determine the overall framework within which PETs operate. They set the legal boundaries. Legislators have the power to draft, amend, and enact laws. Their decisions affect how Privacy-Enhancing Technologies can be used to comply with privacy laws [35]. Judges can steer the law in certain directions with court decisions, filling in the often vague language of the law.

> It lacks court rulings, for practical work. This then, fills it properly. (I-7)

Therefore, the role of lawmakers plays a critical role in guiding legal experts in the usage of Privacy-Enhancing Technologies. Legal experts need to follow the latest laws, regulations, and guidelines that influence the use of Privacy-Enhancing Technologies for data privacy compliance. Also, they must have the ability to interpret court decisions and understand their impact on the use of Privacy-Enhancing Technologies for data privacy compliance.

Supervisory and Regulatory Authorities

> The regulatory authorities rather, because, of course, they have the interpretation of the law. (I-12)

These agencies monitor and enforce privacy. They control that organizations are properly complying with privacy regulations. They also provide advocacy in cases of doubt. The legal experts can work with the authorities when there is ambiguity about a processing operation. "*So we have a very cooperative working relationship with the data protection authorities.*" (I-8) When data is misused, it is the authorities who set the fines. Overall, legislators and regulators define the legal framework within which legal professionals can operate. Their role is critical in policing compliance.

PET supplier

> You have the manufacturer of a product, and you have the data protection legally responsible. That is not always the same as one of the data laws is really responsible. (I-6)

These suppliers provide the actual PETs that are used by the organizations. They often act only as "processors" and the organization as the responsible party, referred to as the "controller"[7]. This can lead to liability issues. Legal professionals need to draft contracts with these suppliers and ensure they meet certain legal requirements. This may include the use of "appropriate technical and organizational measures" [7].

> The ruler of the software is not the one who processes the data, but I am, as the company, because I enter the data of the employees. (I-6)

5.2.1.3. Technical Experts

Technical experts play an important role in ensuring data privacy compliance when using Privacy-Enhancing Technologies. PETs are considered by the technical department during the design phase of a new product. At this stage, collaboration between technical and legal experts is critical to ensure that the implementation meets all legal requirements [32]. Therefore, the most important collaboration is the technical-legal one. This is discussed in more detail below.

> Simply what one exchanges their times. And most of the time, that's data protection and IT, so those are the two main roles that always play a role. (I-5)

Most legal experts worked with the information security or general IT development teams. In this paper, I will often refer to the technical experts in general, but their role varies from organization to organization. Technical experts ensure that legal requirements are incorporated into the design of a system and that Privacy-Enhancing Technologies are

implemented correctly. In addition, technical experts are essential in helping legal privacy departments to evaluate new technologies, such as PETs:

> I have a lot to do with them, then I have an exchange with their information security, often a direct, that I say, okay, we have new software, for example, and these technical and organizational measures are used. Have you already checked them? Should we check them? Do we check them together? Do we coordinate our efforts? (I-8)

Looking at the process of implementing Privacy-Enhancing Technologies, the collaboration between technical and legal experts is closely linked from the very beginning. In the first steps, they provide technical guidance in understanding the complexities of new IT products. "*If they are complex technical issues, complex systems, then we are actually very close from the start. So, then I have it explained to me, also from the side of how it works in simple language, so also lawyers can understand. I would say that the more complex and the more technical the processing procedure is, the quicker the cooperation with the IT people will be.*" (I-8)

At the same time, the legal experts must educate the technical experts about the legal requirements for the new processing activity [19]. Finally, they must integrate the legal requirements into the technical specifications. Therefore, it is important to discuss the key requirements to fulfill the mandate of Privacy by Design and to ensure a data privacy-compliant product. Article 5 and its data protection principles are very the key reference in this process, as well as the specifications of technical measures in Articles 25 and 32. These must be met by the implementation [9]. Fulfilling these legal requirements and at the same time developing well-functioning software without too high costs can be a great challenge for developers [27].

In cases where there are uncertainties on the technical side, legal experts can help with legal advocacy. They can evaluate potential risks associated with the use of certain PETs and provide a legal assessment. One interviewee also says that in the beginning he often spent hours with the faculty just explaining "*how it works*" (I-6) and trying to understand how it "*can work from a legal standpoint.*" (I-6)

In selecting and evaluating Privacy-Enhancing Technologies, one respondent mentioned: "*So I am 100 % dependent on my colleague from IT.*" (I-8) Privacy-Enhancing Technologies are mostly proposed by the technical departments. In one organization, there was a dedicated information security department that had a kind of "*radar function*" (I-8) to look for the latest industry standards that meet the requirements of the state of the art. They look to regulators and industry standards for guidance. Mostly the technical department "*makes sure that they use the latest technology that makes sense.*" (I-8)

> Well, it's often like this: you've read something somewhere that's supposed to be great, and you ask IT, wouldn't that also be something for us? Yes, well, but I'd say not in our big company because they're so far ahead. I can't tell them anything new. (I-8)

After a product is finished, it still must be monitored from the technical and legal side. There can be the need to adapt to new legal or technical developments to stay privacy compliant. This can lead to a completely new review.

> Yes, that's also the point, that when I introduce something new, that we already have some tool that works well and they bring out something new, that they then also want to use, that you then have to go through the whole process again. (I-5)

5.2.2. Proactive

To guarantee that legal experts can support the usage of Privacy-Enhancing Technologies, they must fulfill proactive tasks and responsibilities. Legal experts need to have regulatory expertise related to PETs. They are responsible for following the latest developments and informing their technical colleagues of the latest developments. They are also responsible for interpreting regulatory requirements for specific use cases. They are the ones who bridge the gap from regulatory requirements to technology and its applicability to the business. When new rulings come down, they must consider how that ruling might affect the organization's use of PETs. Legal professionals also need to build organizational structures to support the privacy compliance process when using PETs. Legal professionals need to develop privacy policies. These documents are regularly updated to reflect evolving regulations. They serve as the foundation for the organization's position on privacy. They guide internal processes and set expectations for third parties.

5.2.3. For a New Product

PETs should be considered at the software design stage [21]. Legal experts support the selection and implementation by bridging the gap between the technical implementation and the legal requirements.

Understanding the Facts and Regulation Mapping

At the beginning of the development of a new business solution, the legal experts must understand every detail of the new product and the respective regulations:

> We want to understand exactly what is supposed to be done, because, of course, everything depends on that, that you understand it and that is always one of the hardest or most complicated parts. (I-5)

They often talk about "*analyzing the facts*" (I-8). Legal professionals need to understand what is being done with the personal information at each stage of the processing activity. (Table 1) This means understanding the collection, storage, use, and destruction of data.

One interviewee describes this process as "*phase of forensics where we explain or clarify and have it explained to us how the system works.*" (I-8) They need to understand the system to an extent that they can make a legal assessment of the new case. In response to the question of what exactly they need to know for their judgment, one interviewee mentions: "*We need to understand the life cycle of the data, from birth to death.*" (I-8) Furthermore, it is mentioned: "*I don't really care what the system is called and how exactly it works in the background, as long as I understand how the data processing works.*" (I-8) One interviewee says: "*The whole evaluation stands and falls with the analysis of the facts. If the facts are not really explored, then it will be super difficult to evaluate. In other words, to assess it solidly.*" (I-8)

> We cannot give good advice because we don't know the technology. That is the issue. I can't say from the beginning that you have to do this and that. We need a bit of fodder first. We first must know what this product should look like, and then we can look at it. (I-1)

For understanding and analyzing the technical aspects of a new product, input from the IT department is essential, as discussed. Once the facts have been understood, the legal experts carry out a regulatory mapping and analysis. This process can vary from organization to organization and from legal expert to legal expert. One interviewee describes this process as "*overlaying*" (I-8) the legal requirements on top of the facts, thus aligning all the necessary laws and regulations with the new product. It was also mentioned that due to the differences between each case, the mapping is also very different. Two legal experts mentioned that they work according to a "*mental checklist*" (I-5) in this process. With each new product, they start from scratch and work their way down the list step by step.

This can include a variety of legal considerations. Beginning from the lawfulness of processing to being accountable. One interviewee, when asked about his approach to regulatory mapping, explains: "*Article 5 of the GDPR is always a good benchmark for me. And that's where I'm really going through it on the basis of the existing facts.*" (I-8) (Table 2)

In this context, legal experts can also inform the technical departments of the legal requirements for data privacy compliance. Mentioning the mandate of Privacy by Design at the beginning of a project can be essential for a later consideration of Privacy-Enhancing Technologies.

Risk Assessment

Article 25 of the GDPR mandates the implementation of "appropriate technical and organizational measures" [7], considering the varying likelihood and severity of risks that might arise on the rights and freedoms of natural persons due to processing activities [33]. In this context, the responsibility falls on legal experts to conduct a comprehensive risk assessment to determine the necessary security measures. This risk assessment is the basis for the later selection of the right Privacy-Enhancing Technology. One interviewee describes this process:

> We say we have now grasped the facts, we have a legal basis, and there is no showstopper where we say it is not possible at all, but of course, we still have to recognize and assess the risk somehow. (I-5)

In the GDPR risk is defined as an event that could harm "the rights and freedoms of natural persons" [7]. The determination of "the likelihood and severity of the risk" must be analyzed in relation to the nature, scope, context, and purposes of the processing [7]. Legal experts must identify, analyze, and classify these risks. This process is integral to safeguarding individual rights.

The risk assessment functions as the basis for evaluating the necessary measures to mitigate potential threats.

If the initial risk assessment concludes that the new processing activity is likely to pose a high risk to individuals' personal data, a Data Protection Impact Assessment (DPIA) must be carried out by legal experts [33]. One interviewee describes this process for a PET as a service provider:

> In the DPIA you really have to look at it step by step, that you say how the service provider acts. He should put up his infrastructure, and because of that you also involve the IT person, because he will then show his infrastructure and then describe to him exactly what he does. And then you can also find the points where actually the high risk is because most of the time that's not the whole process. (I-5)

As mentioned above, the DPIA involves a systematic description of the processing operations, including the purposes of the processing and a careful assessment of the necessity and proportionality of these purposes [33].

By identifying exactly where there is a high risk in the processing activity, you can identify the right Privacy-Enhancing Technology to address these issues at that stage of the process. The selected technology must reduce high-risk processing activities to a low level, thereby ensuring GDPR compliance and enhancing data protection.

Assessment and Selection of Privacy-Enhancing Technologies

After a risk assessment, appropriate technical and organizational measures must be implemented to reduce the residual risk to a remote level [33]. As discussed, Privacy-Enhancing Technologies can serve as such technical measures. However, to use them, legal experts need to know and understand at what stage of processing they can be used. This is a prerequisite for assessing them for risk mitigation. You need to be able to match a specific PET to a risk identified in the previous step. One respondent mentioned that the most important knowledge for selecting and assessing PETs for risk mitigation is to know what you can use them for. It is essential that you propose "*measures that fit*" (I-8). One interviewee describes

"*you have to offer the solution to a problem.*" (I-5) In our case, "*for which problems the respective PET solutions are*" (I-5) That is why the findings of the risk assessment are so valuable. In the risk assessment, you have worked with the technical department to identify the processing steps that pose the greatest risk. So, you can better assess at which stage a PET can be used or which PETs can be combined.

In the case of a third-party supplier, there are several other legal considerations. Legal experts must determine the data protection roles. As introduced before, although PET supplier has developed the technology that processes the data, the organization that functions as the controller has the responsibility to guarantee that all legal requirements are fulfilled [35].

By choosing the right PET for the right problem, they can act as a risk mitigation measure. Article 32 of the GDPR deals with the security of processing. It states that "technical and organizational measures shall ensure a level of security appropriate to the risk" [7]. This means that in the end, the data privacy compliance team must explain how the implemented technical measures lower the residual risk to a remote level:

> This is where these Privacy-Enhancing Technologies come into play, and one then says, yes, the risk is high or present. And with these technologies, I no longer have a high risk. (I-5)

Also, when assessing technical aspects, several other aspects need to be considered: the state of the art, the cost of implementing the protective measures, the nature, scope, context, and purposes of the processing, minimizing the threats to the rights and freedoms of individuals from the processing [7]. All are mentioned in Article 25 of the GDPR, as discussed in chapter 2.

Another guideline for assessing the appropriateness of the chosen PET, pseudonymization, and encryption, is mentioned in Article 32 [7]. In this context, a legal expert also mentioned a difficult challenge. Often, encryption specifications can change rapidly:

> So, I call that for encryption length. We had a time, there was 128 enough. Today or the point is today, the BSI still says 128 is enough, but the recommendation is 256. With the result that the supervisory authorities say that 128 is no longer sufficient. (I-3)

As a result, legal professionals must keep abreast of the latest developments in encryption technology to ensure that the Privacy-Enhancing Technology chosen is "appropriate" [7].

Legal practitioners also need to be able to assess which data protection principle can be achieved using Privacy-Enhancing Technologies. With respect to the technical design of a system, in particular, the principles of purpose limitation, storage limitation, integrity and confidentiality, data minimization, and accuracy become relevant [9]. Again, it is very important to work with the technical departments to understand which technologies can help achieve each principle and how they do so.

In the end, legal experts do not need to understand exactly how the technology works, but they do need to have people who can explain the functions to them to the extent that they can make their legal judgments about how the technical measure reduces the risk to a remote level, and they need to be able to argue why its use is appropriate. One interviewee describes the extent of knowledge as:

> So, you have to give me as a faculty or also the techies so much fodder in my hand that I can say, okay, I can argue that legally in front of a supervisory authority. (I-8)

Most of the time the technical experts propose new technologies as PETs. They search for guidance from the supervisory authorities and industry standards. Mostly the technical department "*makes sure that they use the latest technology that makes sense*" (I-5). One interviewee explains in this context: "*(The technical experts) also really have another technical know-how that they know what this technology can achieve somewhere at this time. It can only be that we provide the food for thought.*" (I-5) One interviewee describes the process of assessing a new technical measure in collaboration with his information security officer:

> What is this anyway?
> And is that good?
> And is that state-of-the-art?
> The IT guy tells me then, now it's like this.
> Fits. There's a catch. (I-5)

In smaller and medium-sized organizations, it is more common for legal professionals to come up with ideas for new technologies. One interviewee says: "*When I was still a data protection advisor in the office, some people say, 'Hey, you've had this problem before, I read that there was something new.'*" (I-5)

After selecting a Privacy-Enhancing Technology, legal experts then need a "*basic understanding*" (I-8) to build a bridge to the data protection laws and regulations. So, they must use the technical input, to argue how the technical measure can achieve data privacy compliance legally. This kind of argumentation is usually carried out within the documentation and is important to defend the chosen measures in front of a supervisory authority.

It is also important that the use of PETs does not increase the risks of processing. In other words, it must be assessed in a very concrete way whether the use of PETs leads to more advantages than disadvantages:

> So, the bottom line is, I would also say that it is necessary to introduce measures to the extent that it makes sense. So that the Privacy-Enhancing Technology does not become a risk somewhere because I use them blindly. (I-8)

When high-risk scenarios are identified, legal experts can seek consultation with regulators to ensure appropriate risk mitigation. If the high risk persists after organizational and technical

measures have been implemented, the supervisory authority must be consulted [33]. They work together to identify appropriate technical and organizational measures that can reduce medium or high risks to a remote level. This proactive approach helps ensure compliance with data protection regulations and builds trust between companies and regulators.

Scaling and Adjustment

In most cases, the work of legal experts in supporting the data protection compliance process is completed after the selection and assessment of the Privacy-Enhancing Technologies. So, after the requirements analysis and the go-ahead, in most cases, the work is done:

> You define it, you discuss it, with the IT department, but then it's actually up to them. (I-8)

> It can be, but basically, because there is also a lack of capacity, it is like this: you give the direction, by saying what is to be used and implemented. (I-5)

In some cases, when there is a complex technology and case, there is the need for further guidance during the process of implementation. "*It may be that you sit down together again and recalibrate it and shape it and then actually make risk decisions. But then neither privacy, IT, nor marketing can meet, but they will then escalate in the direction of the management, so that they will say, okay, we now have to make a decision.*" (I-8)

When it comes to Privacy-Enhancing Technologies, it is often a question of scaling [27]. There are many ways to increase privacy with the use of a PET. This privacy-utility trade-off often needs to be discussed during implementation and testing, when you can better anticipate how well your business objective can be achieved:

> Yes, in the context of calibration, of course, it can happen that the data protection officers say, okay, we are going very, very strongly to the right in the context of privacy and then the marketing department comes and says, no, absolutely not. (I-8)

Ultimately, the business judgment rule must be applied, which means that management must decide when the risk is sufficiently mitigated and whether they want to bear the residual risk:

> And yes, at some point, that is the last question of evaluation and that is a question of where the legal expertise comes in, where the technical expertise comes in. And at the very end, it's the business judgment rule again. The decision is made by the one who uses it. Neither the computer scientists nor we lawyers can take that away from them, the personal responsibility for what they do. We can give him definitions, and terms of definition. In the end, we will always have to say that maybe there is someone else who sees it differently, and you have to accept that risk. (I-3)

In some cases, organizations also consult the supervisory authorities when there are uncertainties in the implementation. One regulator describes this:

> But it still happens relatively often, at least that's my perception, that companies approach us even before they do something. There are certainly also many companies that don't do that. But we order relatively often when there are uncertainties, they come to us and ask us, okay, is this enough? (I-7)

Documentation and Proof of Compliance

Data privacy compliance documentation is an integral part of the data privacy compliance process. "*But that's also to say that I do at least 90 percent of the work that is done in the context of documentation.*" (I-4) Ultimately, the documentation of the data privacy compliance process can serve as proof of compliance to a supervisory authority:

> The second part where the lawyer comes into play, that's the documentation issues.
> If you think that all the documentation in the end, yes, one must say, for the supervisory authority.
> It is important that lawyers look at it to understand whether it is the language that a supervisory authority understands. (I-4)

This highlights an important aspect. Legal professionals also act as advocates for an organization. They must understand the technical, legal, and regulatory language to support the use of PETs. Ultimately, they must make the legal case to an authority or a court as to why the measures taken are "appropriate" [7].

In recent years, regulators have come to expect a more detailed description and assessment of how the specific technical measure can contribute to data protection compliance. They require detailed documentation and an explanation of how data privacy compliance is achieved. One respondent describes this as follows:

> And now, of course, we are also confronted by the supervisory authorities. They send us a hard case and say, we assume this and that and now, dear company, prove me now wrong. [...] So 2018, 2019 the questions were still very basic. So, do they have a data protection management system? Yes. And now they are already asking, okay, how do they implement accountability in the context of the processing? So, they're going into a lot of detail now. (I-8)

Therefore, one legal expert explains that he often adds a detailed description of the chosen technical measures and how they work. It is then also important that the legal experts understand the technical measure and how it reduces the risk to a remote level, in order to be able to explain to the supervisory authorities how the risk is reduced:

> And then it could be that an appendix is added, and it explains what exactly is happening. (I-8)

At the end of the day, it is important that there is a good basis for argumentation and that the regulators can see that you have a privacy policy.

In the case of a third-party vendor who offers a PET as a service. Legal experts must guarantee that they use the PET properly and have technical and organizational measures to ensure data privacy compliance. They are therefore responsible for communication with the providers and conducting contracts where all the legal and technical requirements are stipulated.

This is also important as proof of regulatory compliance to the supervisory authorities:

> Then in the worst case, I could go to court and say,
> That is contractually agreed.
> That's what he did.
> That is not in agreement.
> That's why he started a breach of contract.
> That would then be good for me as a lawyer because then I can grab him right by the ears.
> That's why I always make sure that everything is described in great detail. (I-8)

One respondent mentions that once a particular technical measure has been selected, he asks for a detailed explanation of the technology and how it will be used. This explanation can then be used as documentation and a basis for legal argumentation on how Privacy-by-Design was achieved and how an appropriate level of security for the processing was achieved. One respondent describes this process as follows:

> And then the service provider comes and says, yes, so we have established and taken the following encryption measures, the following measures for pseudonymization, the following measures for the resilience of the information technology systems, etc. Ideally, he would then write me ten pages about it and then I would see that and say, okay, wow, that's already justifiable for me. (I-8)

5.2.4. Continuous Compliance Monitoring

To maintain compliance, legal experts monitor the usage of Privacy-Enhancing Technologies.

> But internally, of course, you must review it, so you are also internally obliged to review your thing regularly, to review your work on a regular basis. If something new has been introduced, it has a big risk. We should look at that regularly every one or two years. And that would be the main point. (I-8)

The legal landscape is also constantly evolving [11]. Legal professionals need to monitor new regulations, legal interpretations, and court decisions that may affect the use of PETs for data protection compliance. This is particularly important because data protection law is a very young and evolving field. Many terms are still open to interpretation and will need to be filled in by case law [18]. In addition, more and more guidance is being developed by regulators, which may also affect the use of PETs. Legal professionals need to ensure that current practices are in line with these developments.

There may also be a change on the technical side, where the legal experts need to assess whether this introduces new risks to privacy compliance or whether new changes need to be made.

> Yes, that's also the point, that when I introduce something new, that we already have some tool that works well and they bring out something new, that they then also want to use, that you then have to go through the whole process again. (I-5)

This underlines the iterative nature of data privacy compliance and the need to review the process from both a legal and technical perspective. They also need to keep each other informed of changes to guarantee that no compliance gap develops.

5.3. Visualization

To answer Research Question 1, the role of legal experts in the process of data privacy compliance with Privacy-Enhancing Technologies for a new product is visualized. The insights on this visualization are grounded in the interviews. There is a special emphasis on the legal assessment of PETs. This is the core of the diagram. Three further interviews for its validation and improvement were conducted. The general supportive tasks are solution strategies that were found during the interviews. These tasks can be performed by legal experts to support the usage of Privacy-Enhancing Technologies in organizations. These tasks will be further discussed in Chapter 7. The legal tasks in the process diagram relate to the development of a new product with PETs and how legal aspects guide this process.

Explanatory Notes

Rhomb: Exclusive conditional gateway.

Unidirectional Arrow: Links activities, events, and gateways within the process.

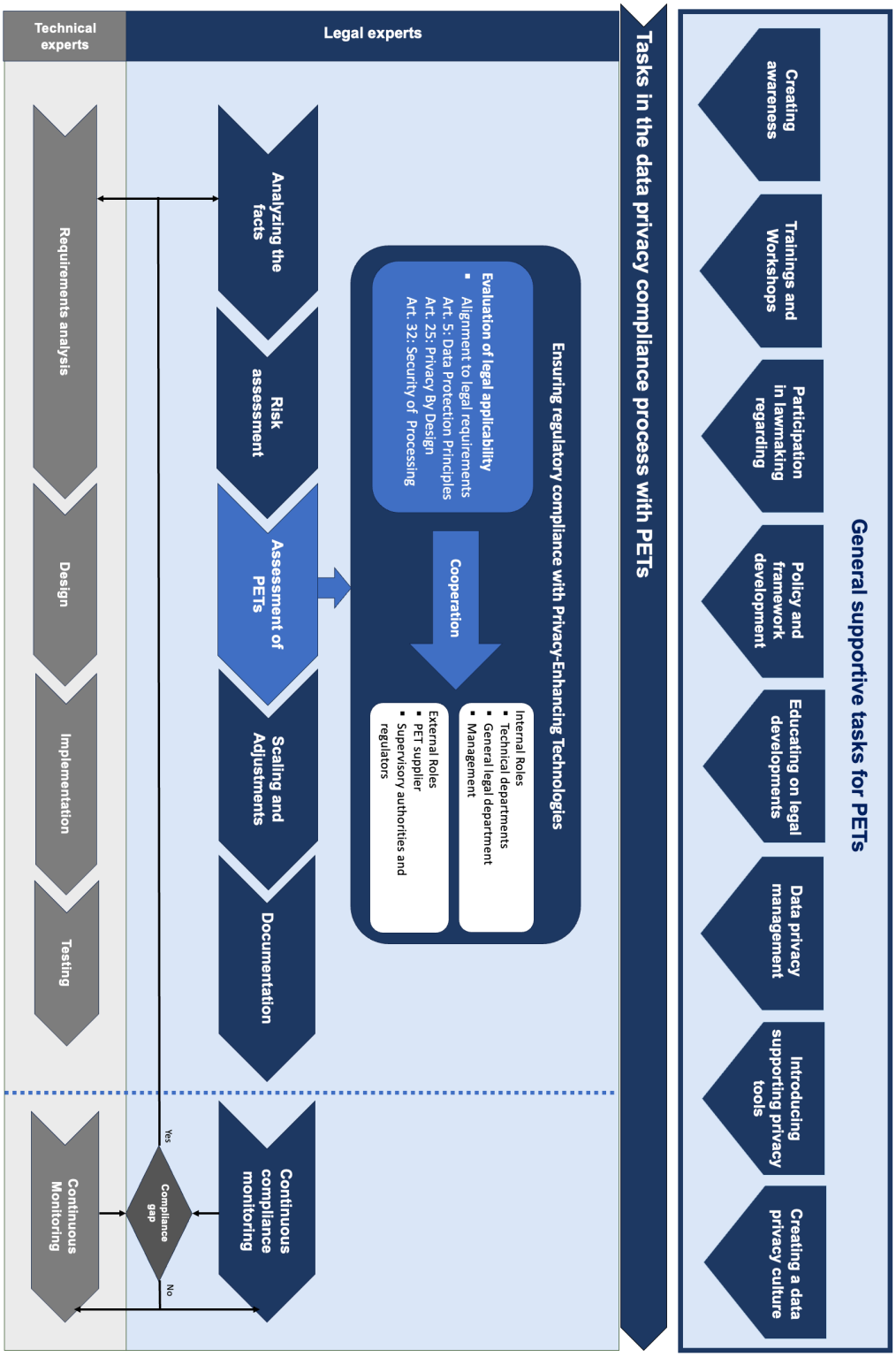

Figure 5.1.: The Role of Legal Experts

5.4. Conclusion

The complex process of implementing and maintaining Privacy-Enhancing Technologies requires an understanding of both the technical and legal aspects.

Legal experts have the regulatory expertise to guide organizations through the complex legal landscape. They must proactively stay ahead of rulings, policies, and regulations to ensure the organization meets legal requirements, even as technologies evolve.

One of the most important roles of these experts is their ability to interpret and adapt legal guidance for Privacy-Enhancing Technologies. This is critical as it enables organizations to translate often abstract legal requirements into concrete technology implementations. In this way, legal experts bridge the gap between data protection law requirements and the implementation of Privacy-Enhancing Technologies for data privacy compliance.

Moreover, their role is not limited to interpreting the law. Legal experts actively work with technical teams to guide the implementation of Privacy-Enhancing Technologies. They ensure that technologies comply with data protection principles and measure their effectiveness against criteria such as risk, state of the art, cost impact, resilience, and availability. This relationship with technical departments is critical, as it fosters a shared understanding of goals and challenges and enables solutions.

Another key aspect of their role is to collaborate with internal stakeholders such as legal, HR, and management. This internal collaboration ensures that all departments within an organization are on the same page and working together to meet legal requirements.

In addition to their internal role, legal professionals also work closely with external stakeholders, particularly regulators. This external collaboration is critical to ensure that the organization is always up-to-date on the latest regulatory requirements and the latest guidelines for using technology to improve data privacy.

In addition, legal experts are central to the organization's external engagements, especially when dealing with third-party vendors. By carefully reviewing contracts and ensuring compliance, they protect the organization from potential breaches and risks of non-compliance.

Another key aspect of their role is that they continually follow the adoption of Privacy-Enhancing Technologies. Because data protection law still evolving, legal experts have to check regularly if the implementation of Privacy-Enhancing Technologies fulfills current legal requirements. Legal experts ensure that the usage of PETs remains compliant with changing laws and the evolving needs of the business.

At the organizational level, their role goes beyond compliance. They are tasked with developing policies and structures that support the seamless integration of Privacy-Enhancing Technologies.

In summary, legal experts are tasked to bridge the gap between technology and law. They must ensure compliance with the law but also enable technological developments. As a result,

they must communicate internally and externally to find the best solutions. By bridging the often complex gap between technology and law, they can ensure that Privacy-Enhancing Technologies help ensure an organization's data privacy compliance.

6. Challenges and Obstacles

This Chapter identifies the practical challenges that legal practitioners face in the process of complying with Privacy-Enhancing Technologies. These challenges are identified from the qualitative analysis of the interviews. The challenges fall into three groups: Regulatory, Technical-legal gap and Organizational. The interviews are supported by direct quotes from the interviews. A discussion is built around the identified challenges.

Each group of challenges is introduced by a table showing the interviews in which the challenge was mentioned and the total number of mentions. Each challenge is then discussed. All challenges contain several direct quotes as a basis for discussion.

6.1. Regulatory and Legal

Challenges	**Mentions**	**Interviewees**
Regulatory and legal vagueness	(I-1) (I-2), (I-3), (I-4), (I-5), (I-6), (I-7), (I-8), (I-9), (I-10), (I.11), (I-12), (I-14)	13
PETs mostly not state-of-the-art	(I-3), (I-4), (I-7), (I-12), (I-13)	5
Applicability of PETs to the Existing Law	(I-3), (I-5), (I-6), (I-10), (I-13), (I-14), (I-15)	7
Case-by-case assessments	(I-1), (I-3), (I-4), (I-5), (I-6), (I-7), (I-8), (I-9), (I-12), (I-15)	10
Liability issues	(I-3), (I-5), (I-6), (I-7)	4
Huge number of laws and regulations	(I-3), (I-5), (I-6), (I-10), (I-13), (I-14), (I-15)	7

Table 6.1.: Challenges

6.1.1. Regulatory and Legal Vagueness

The General Data Protection Regulation states the principle of Privacy By Design in Article 25. It requires the implementation of "appropriate technical measures" to protect personal data [7].

The word "appropriate" alone leaves much room for interpretation. The other specifications of the technical measures, such as state of the art, and reasonable risk, are also open too much interpretation. This leads to challenges in selecting and implementing Privacy-Enhancing Technologies as technical measures. Nonetheless, the vagueness is necessary to track the rapidly advancing technical developments:

> I think the vagueness is intentional because it allows us to capture new constellations. It is also the only way that technology and law can really stay somewhere in harmony because the law is actually quite different, not very dynamic, but rather long-term. (I-2)

Legal experts need concrete examples, standards, guidelines, and case law to evaluate Privacy-Enhancing Technologies legally. They need to bridge the gap from the laws and regulations to the implementation of PETs. They need to be able to argue legally how these technologies can contribute to data privacy compliance in each use case:

> The more it comes, the better it gets with the guidelines, with all the new court decisions that are out there. The more solid it gets, the better. There's a lack of court decisions for practical work. That's what really fills it in and where the lines are drawn. (I-7)

From the interviews, it becomes clear that the lack of case law is a major challenge to the use of Privacy-Enhancing Technologies. The lack of court decisions provides legal experts with little guidance on how to approach the use of Privacy-Enhancing Technologies. Traditionally, legal experts rely on commentary to interpret open legal concepts. As one interviewee says, "*the commentary literature tells us what's meant by that term, they look at what the case law has said about it.*" (I-5) Without these other tools, the GDPR leaves a lot of room for interpretation, and that "*can be understood both ways, both extremes.*" (I-5)

Article 25 can be interpreted in very different ways. "*What is perhaps a bit lacking, where it is really difficult, is the concretization of technical and organizational measures.*" (I-11) This vagueness makes it often difficult for legal experts to assess when the appropriateness is fulfilled, which was for several legal experts a frustrating issue:

> We already had that in the 25, the whole 25 paragraph 1, if you go through it.
> So that's where it starts, under consideration.
> Yeah, what is under consideration now?
> Where are the thresholds? This is all completely unclear.
> If the risks are sufficiently mitigated, no one can say what the cost of implementation will be. It's all undetermined. There are no limits, there are no thresholds. (I-7)

From the interviews, it is clear that the main challenges in evaluating PETs are assessing their risk appropriateness, classifying them as pseudonymized or anonymized techniques, and whether they are state of the art.

Pseudonymized and Anonymized

> There is a bit of a fight about it when something is personal and when it is not. That's actually, from the terminology, the main sticking point when you talk to techies, is it personal, is it anonymous, what is pseudonymous? So the gradation between person-related, where pseudonym has person reference, and anonymous is not person-related. (I-10)

The GDPR recognizes pseudonymization as a method for securing personal data. But there is a significant gap when it comes to distinguishing pseudonymization from encryption and, more importantly, from anonymization [26]. Legal experts must be able to categorize the technologies to legally explain why these technologies are appropriate for the specific use case. Especially the distinction between pseudonymization and anonymization has high importance for legal experts [27]. Anonymized data is no longer subject to the GDPR which can free organizations from large bureaucratic hurdles.

In the GDPR anonymous data is defined as "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" [7]. This leaves much room for interpretation, as also often complained about, "*With anonymization and the specifications for anonymization, you're actually pretty much on your own.*" (I-11)

The classification of Privacy-Enhancing Technologies is therefore also very difficult to this day [9]. Differential privacy, for example, could be considered an anonymization technique [26]. However, so far there are very few guidelines from a regulatory perspective to assess if its use can meet anonymization:

> And that's just a big issue for a lot of people, how do we deal with anonymized data, how does that work, and so on? These are all things that have to be worked out by science regulators and so on. And even now, after five years, there is still a lot of uncertainty in a lot of areas. (I-3)

Risk

The GDPR categorizes risks and distinguishes between "risk" and "high risk" [7]. The technical measures should set the risk down to a remote level [33]. There is often no clear answer on how Privacy-Enhancing Technologies can be used effectively to mitigate the risks of a processing activity. And how it can be ensured that the risk is reduced to a lower level. Without explicit clarity, it is difficult to determine which data security measures are appropriate. This lack of clarity is perhaps best illustrated by one respondent who noted:

> When you look at Articles 25 and 32, you're looking at the nature and scope of the processing, the costs involved, and the current state of the art. All of these factors need to be considered in order to make an accurate risk assessment. However,

> there is no standard methodology, even among the authorities, which makes it difficult to have a consistent assessment. (I-12)

Another aspect of this challenge is the need for more guidance from regulators. As one interviewee put it, "*Article 32 allows for some grading of risk levels, but the challenge is that regulatory approval is critical.*" (I-6)

6.1.2. PETs Mostly not State of the Art

The term state-of-the-art often comes up in discussions about Privacy-Enhancing Technologies. However, there is often unclarity about the current state-of-the-art and what qualifies a Privacy-Enhancing Technology as state-of-the-art. The views can additionally often differ between different sectors:

> Yet its interpretation in academia stands in stark contrast to its practical, official application. (I-12)

Legal experts often rely on their technical departments to provide clarity. But even among these experts, the definition of what exactly constitutes state-of-the-art is sometimes uncertain. When integrating PETs for data privacy compliance, the main question is how mature they are and what is considered state-of-the-art. While the term state of the art is often used, it is still not clearly defined what qualifies a technology to fall under this term. There are different classifications for technologies, as one respondent mentions:

> There's the current state-of-the-art, the current state-of-the-science, industry standards, and established industry standards. That's what you always must tell engineers. It's not the same thing. (I-3)

This quote underscores the challenge, of distinguishing what is new and innovative from what is established, tested, and reliable. Legal experts who must ensure the organization's data privacy compliance must ensure that the technology is current industry standard or proven and reliable. They must ensure that the organization is always in compliance with the law and not using insecure technology. While certain Privacy-Enhancing Technologies are state-of-the-art in academic circles, they have yet to catch on in legal practice [9]:

> We don't do things like Homomorphic Encryption or Differential Privacy. Because that means they are not state-of-the-art in our sense. (I-12)

It was added: "*Privacy-Enhancing Technologies are currently state of the art mainly in academia, but not in privacy compliance practice. Someone has to build systems that are available in the marketplace.*" (I-12)

The gap between the academic appreciation of PETs and their practical application in privacy is wide. This underscores the central role of industry in bridging the gap between innovative technologies and practical, scalable solutions, as one interviewee pointed out:

> Someone must build systems that scale for large enterprises, for big data, and for different databases. And until those solutions are available and mature, unfortunately, they don't play a role in government practice. (I-12)

PET supplier should be leading the charge to develop PETs that are state-of-the-art. But this effort is not without challenges. As technologies evolve, the criteria for state-of-the-art-must also evolve. As one interviewee put it: "*That's why I don't know anything about government. Just because what you write today may be obsolete the day after tomorrow.*" (I-12)

6.1.3. Applicability of PETs to the Existing Law

A major challenge is the lack of clarity about the concrete applicability of Privacy-Enhancing Technologies for data privacy compliance. A critical step in the adoption of Privacy by design and PETs, is the demonstration that these instruments can satisfy relevant legal requirements. Ultimately, there needs to be a high level of motivation to implement these complex technologies and to commit the resources to do so. One respondent says that the most important knowledge for selecting and evaluating PETs is to understand what they contribute to privacy compliance:

> What is it, what is the consequence of using such a technology? Namely on the applicability of data protection law, and the applicability of processing. (I-4)

This shows that there is a challenge for legal experts in the lack of clarity regarding their contribution to data privacy compliance. This problem stems from the lack of a practical legal evaluation of PETs for data privacy compliance. As highlighted by the statement, "*I mean, if it's not available on the market and it's not being used, no lawyer is going to stand up and say I'm going to evaluate it. It's difficult because we're testing the real world, computing, and we can only test what's being used, and if it's an academic prototype concept somewhere, it's not going to get a legal evaluation.*" (I-12)

This legal evaluation would include an assessment of the open legal terms mentioned above, but also measurement against the data protection principles that are at the heart of the GDPR. These principles can sometimes be high-level and open to interpretation. Any processing activity should comply with these principles, and technical measures should be measured according to these principles. Therefore, mapping to these data protection principles should also be achieved. Ultimately, it is challenging to determine whether a PET meets the intent of the principles, so the implementation of a PET itself must also be considered. Understanding how these technologies can support privacy principles requires close collaboration between technical and legal experts. A deep technical understanding is needed to answer questions about data minimization, storage limits, or accuracy.

In general, there is a great lack of clarity about the legal applicability of PETS, but also for which scenarios they can be used. This knowledge is important for legal experts to assist in the selection of PETs and their use. While certain PETs may appear to be applicable to

certain situations based on regulatory recommendations or approvals, their applicability may vary drastically depending on the context. For example, a PET that is appropriate for one use case, such as encryption in international data transfers, may not be appropriate for another, even if the scenarios seem similar. Such situations challenge the lawyer's ability to ensure compliance in different scenarios.

6.1.4. Case-by-case Assessment

The use of Privacy-Enhancing Technologies can help ensure compliance with data protection regulations. However, legal requirements and interpretations often depend on the context and specifics of the data processing. This makes it difficult to develop guidelines that are universally applicable. Regulatory frameworks must consider many factors, which, as mentioned earlier, are not precise. Developing policies that cover all possible scenarios can be impractical and restrictive. In addition, they may not address all the use cases for Privacy-Enhancing Technologies. Therefore, it is important to really understand the details of each case to figure out what PET can be used and how it should be implemented to ensure data privacy compliance:

> That's the problem we always have in consulting. You always have to say that nobody in the legal field wants to hear that, but it always depends on the individual case, on the specific processing, and then you have to see if it works or not. (I-7)

This poses significant challenges, particularly with respect to Privacy-Enhancing Technologies. Difficult decisions have to be made not only about which PET to choose but also about how to implement it:

> Yes, but that too, I have to come back to that earlier, that is a case-by-case decision. I have to take a very close look at the processing operations, what kind of data is being processed, and what are the dimensions of these data sets, and only then I can somehow make a decision about which technology to use with which attributes and under which conditions. (I-12)

Every use case is different, so the legal professional cannot rely solely on standards and guidelines. They can only provide some guidance, but legal professionals must make the final assessment of each case. This requires a basic understanding of the technologies and their legal implications.

Another aspect is that legal experts must ensure that legal requirements are met, but also that the system can function properly. This also means making sure that innovation is not hindered by privacy. There are several aspects that need to be considered in their decisions, which have different implications for each case. Legal experts must always find a compromise to ensure proper implementation while not restricting the business. This requires legal experts to understand the technologies and their different implementations.

6.1.5. Liability Issues

When integrating Privacy-Enhancing Technologies for data privacy compliance, legal experts are concerned about the issue of liability. The maturity and availability of PETs from well-established suppliers is important. There needs to be a high level of reliability to support the use of PETs. "*However, as far as I know, there is no commercial supplier that really has it on the market*" (I-3) This limited availability raises questions about the readiness of these technologies for real-world use.

The GDPR identifies different roles in the processing activities, the data controller and the data processor. The controller determines the purposes and means of processing personal data [7]. The data processor processes the data on behalf of the controller [7]. When PETs are used as a service, liability issues may arise. The processor is not the controller. Under the GDPR, the controller is primarily responsible for ensuring compliance with data protection regulations. Therefore, contracts between controllers and processors are required to outline their respective responsibilities to ensure that the use of PETs can help ensure data protection compliance.

In the context of PETs, the issue of liability becomes very important, as functional errors could potentially lead to data breaches or violations of data protection regulations. If a PET leads to data breaches, the data controller will have to deal with the legal and regulatory consequences:

> And the person responsible under data protection law, which is me, the company, has to comply with data protection law, not the person who developed the software. (I-6)

To minimize the risk of non-compliance, legal professionals need the assurance of a stable, mature product from a reliable vendor. Choosing a well-established PET vendor is critical to minimizing potential risks.

6.1.6. Massive Amount of Laws

The legal landscape for Privacy-Enhancing Technologies is not only impacted by rapidly changing national regulations but is also heavily influenced by the different regulatory frameworks that exist in different countries. Each nation has its own set of regulations, standards, and compliance requirements:

> The compliance requirements are going to increase significantly in terms of data. The demands, the requirements are extremely high, and the push in the compliance center will increase significantly. (I-6)

For corporations and organizations that operate across borders, the challenge is to navigate this complex regulatory landscape. It is about achieving data privacy compliance in multiple countries, each with its own regulations. One country may accept a PET as compliant, while another may not.

This international disparity can significantly complicate cross-border data transfers. Transferring data from a country with softer privacy laws to one with more stringent regulations can carry compliance risks for PETs. Therefore, the European Union wants to create a consistent regulatory environment with the help of initiatives such as the European Data Strategy [47], the Data Governance Act [48], and the Digital Services Act [49]:

> They want to create this single market for data, but they also want the data space in Europe to facilitate the free flow of data and data traffic. So, it's clear that legislation is shaping the data space. (I-6)

This leads to several regulations and laws that legal experts must consider regarding Privacy-Enhancing Technologies, making their assessment more complex. On the other hand, the motivation and need for these technologies will grow to remain compliant in this regulated landscape. It is a challenge for legal experts to follow the latest legal developments and incorporate them into an organization's privacy compliance.

6.2. Technical-Legal

Another significant area of challenge is the gap between technical and legal world. Technical and legal experts often speak different "languages", making collaboration difficult.

Challenges	**Mentions**	**Interviewees**
Difficulties in interdisciplinary collaboration	(I-1), (I-2), (I-5), (I-7), (I-10), (I-13), (I-14), (I-15)	8
Lack of awareness for PETs	(I-1) (I-2), (I-3), (I-5), (I-6), (I-9), (I-11), (I-14), (I-15)	9
IT-security vs. data privacy	(I-5), (I-7), (I.11), (I-17)	4
Insufficient Technical Expertise	(I-1) (I-2), (I-3), (I-4), (I-5), (I-6), (I-7), (I-8), (I-9), (I-10)	10
Different Dynamics of Law and Technology	(I-3), (I-5), (I-6), (I-10), (I-13), (I-14), (I-15)	7

Table 6.2.: Technical-Legal Challenges

6.2.1. Difficulties in Interdisciplinary Collaboration

Different backgrounds, terminologies, and mindsets of technical and legal experts make the interdisciplinary collaboration difficult.

> This is a challenge for me as a lawyer, of course, because it requires that I can do it and that I understand it. So, it's not the English language, but the technical language. (I-3)

Legal experts are often overwhelmed by the complex mathematical and cryptographic aspects of Privacy-Enhancing Technologies. Legal and technical experts often use the same word differently. Overlooking these differences can cause confusion [10]. As one interviewee put it, "*Between lawyers and IT professionals, it's basically a matter of language and understanding*" (I-14) This "language" includes not just definitions, but deep technical concepts that are not difficult to understand for legal experts. "*It becomes tremendously mathematical. It's really the language of technology that becomes a stumbling block for lawyers,*" (I-11) is said in another interview. On the other side, IT professionals must understand the legal requirements to some extent. They need a clear understanding of the legal requirements in terms of Privacy By Design to ensure that their technical solutions meet the respective data protection requirements. One interviewee points the difficulties in a technical-legal collaboration out:

> For me, this is the biggest gap that we have because lawyers are not used to understanding technology and IT guys will never know everything, they have to know about the law in order to check if their systems and their measures are enough. (I-13)

An understanding in both directions is therefore critical. Legal professionals need to understand the core functions and capabilities of Privacy-Enhancing Technologies, and technologists need to understand the legal requirements that drive the adoption of these technologies. As one expert noted: "*So, to make a legal step understand to technology guys is a difficult job and then vice versa.*" (I-13)

At the heart of the challenge is the need to connect two fundamentally different professional mindsets. What may be clear in that one domain can be ambiguous in another, resulting in potential misunderstandings even when experts believe they are in agreement [10]. While legal experts are concerned with compliance, preserving rights, and avoiding liability, technologists are driven by innovation, scalability, and functionality. Achieving this balance requires communicating and understanding. Initial efforts such as the Standard Privacy Model are a good start [33], but day-to-day interactions require practical and communicative solutions to bridge these two worlds.

6.2.2. Lack of Awareness for PETs in the Legal Function

Privacy-Enhancing Technologies may seem familiar to technical experts, but it was clear from the interviews that there is still a lack of awareness for these technologies. One interviewee emphasized:

> Is this an issue among your colleagues? You know, it's usually driven by the technical side of the business. (I-15)

When asked about Privacy-Enhancing Technologies, many legal experts were unfamiliar with the term. Despite its relevance, the term seemed almost foreign. This was not an isolated case but occurred in almost every interview. This highlights the lack of awareness and understanding of Privacy-Enhancing Technologies within the legal community. As one participant noted, "*the term [Privacy-Enhancing Technology] played virtually no role in day-to-day work*" (I-6).

One possible explanation lies in the academic nature and inherent complexity of Privacy-Enhancing Technologies [23]. Such technologies, with their complex terms and concepts, have not yet found a firm place in everyday legal practice [22]. Interestingly, the legal sector is already using technologies such as access control that fall under the umbrella of Privacy-Enhancing Technologies but are not recognized as such. This discrepancy between academic and practical definitions of PETs widens the gap. One participant noted, "*It is difficult to define the term privacy technologies from a legal perspective because there is no standard definition. It is indeed a broad term.*" (I-1)

To date, there is no real classification or definition of Privacy-Enhancing Technologies, which makes it very difficult to communicate [40]. There is a gap in finding the right explanations for these technologies. Even among larger organizations, where one would expect more technological understanding, awareness for Privacy-Enhancing Technologies remains low. Most of the awareness come from the IT sector. One respondent says, "*There is a lot of understanding of Privacy-Enhancing Technologies in the IT department. Lawyers know they exist but are often not well-versed in their implications.*" (I-12)

These data underscore an urgent need. Knowledge transfers regarding PETs from the technical level to legal departments is needed. Collaboration is the way forward. By combining technical skills with legal expertise, the true potential of Privacy-Enhancing Technologies can be effectively realized.

6.2.3. IT-Security vs. Data Privacy

The synergy and sometimes, tension, between IT security and data protection, can be a problem for legal experts in supporting the usage of Privacy-Enhancing Technologies. Both fields interplay with technology and law. IT security is the foundation for data protection

measures. Data protection cannot exist without IT security. If data is not secure, it cannot be kept private.

> Let's call it Hate-Love, yes. So it is of course the case that IT security goes hand in hand with data protection. That both want to achieve the same thing. However, there are also cases where the two are completely opposed to each other. (I-5)

There is on the one hand the challenge that they can have different objectives. IT-Security primarily revolves around safeguarding data and systems against unauthorized access, tampering, or destruction. Its core goal is to ensure data integrity, confidentiality, and availability [34]. Data privacy, meanwhile, focuses more on how data is collected, processed transferred, and stored. It ensures the rights and privacy of data subjects.

Sometimes there can arise conflicts due to their different objectives, as one interviewee mentions:

> In the end, it is important and makes sense to combine the two, one without the other is not possible. Or rather, data protection is not possible without IT security, but not in every area.
> So sometimes, but rather more rarely, they also oppose each other. (I-6)

In some cases, for example, it can be beneficial to collect more information for IT-security, because this can help to identify potential threats for a system. Data protection on the other hand follows the data protection principles, which also mandate to minimize the data collection to protect the rights and freedom of everyone.

This challenge is very important because in most organizations legal experts are working together with technical experts from the IT-Security. This became clear in almost every interview, one interviewee mentions for example: "*If I have a question like that, I always, always, always ask the cybersecurity team.*" (I-1) These technical experts are armed with deep knowledge about safeguarding data from external threats, but they might not always be skilled in data protection regulations. This can lead to a gap between the legal obligations and the technical implementation.

Legal experts must be aware of this difficult relationship to educate Information security specialists about the additional technical requirements for data protection.

6.2.4. Insufficient Technical Expertise

Legal experts do not need to become technical experts themselves, but they do need a basic understanding of PETs. This is essential to be able to work with the technical experts and to be aware of certain pitfalls in the implementation of PETs for the data privacy compliance process. They will also be better able to assess their legal application and to argue before supervisory authorities how the selected PETs can contribute to data privacy. On the other hand, there are voices which say that legal experts do not need the technical knowledge

themselves, but the right person to ask for it: "*So to have that involvement, okay, you don't need to have the training yourself, maybe you always need to have somebody you can ask and where you can get it from.*" (I-14)

Other legal experts argue that a basic understanding of the technologies is essential to ensure that they help with data privacy compliance. It also reduces the reliance on the technical side when evaluating new technologies, which is especially important for organizations that do not have the technical expertise in-house.

> We cannot just rely on the IT people. I think the lawyers would have to be more persuasive in terms of learning, you know, IT, than the other way around, you know. But that takes time. (I-14)

There is a lack of specialized training materials that explain PETs from a legal perspective. This makes it difficult for legal professionals to educate themselves about these technologies and their privacy implications. This self-education is very common in the legal field and is mentioned several times:

> But you get cases, or you get into areas and you work your way into it through self-study. (I-4)

> With lawyers you have to say, I don't know how much, I haven't studied that much now, but from my own experience or what I've heard, lawyers have to do a lot of self-studies. (I-5)

This lack of educational material prevents legal professionals from learning about PETs. This gap needs to be filled to ensure good cooperation between the technical and legal communities. Clear and good communication can only be achieved if there is a common basis of information. The question of the depth of knowledge that legal experts need to know is answered very differently. It is often mentioned that they needed to know enough to ask the right questions.

> I need to understand enough so that I know when to ask questions and that I can use that to say to supervisors, I understand your question and I know who can answer it and I'm gathering it now. I don't have to know the answer myself. (I-3)

Even for legal experts who want to understand every detail, there comes a point where there are limits. One lawyer says that at a certain point, the technical-legal discussion comes to a point where technical experts and legal experts are unsure. For example, he mentions:

> When it comes to, say, ten bits of personal information per query, do we have a personal reference here or not? (I-7)

The rapidly evolving nature of PETs exacerbates this challenge. Not only are the technologies themselves changing, but so are their applications and integrations across industries. Privacy-Enhancing Technologies in general are evolving rapidly. Legal experts need to ensure that they

are aware of the legal implications of the latest technological developments. It is not enough to understand the technology as it exists today. Legal experts must engage in continuous learning to identify potential legal challenges posed by PETS and be prepared to guide their clients through new developments.

6.2.5. Different Dynamics between Law and Technology

The legal sector is very traditional and long-lasting by nature. This contrasts with the rapidly changing technical world. This discrepancy is a challenge for legal experts who must bridge the gap between law and technology [10].

One legal expert commented, "*So some of the legal education is very peculiar and, well, not very adaptable*" (I-9). The legal sector is very inflexible. This guarantees that laws and regulations can last long and steadfast, but it can hinder to follow of the newest technological developments. The traditional legal structure is difficult to connect with the rapidly evolving field of Privacy-Enhancing Technologies. Also, the legal education is very traditional. As one of them notes, "*law school is actually a very traditional and very conservative education*" (I-5). This makes the integration of technical knowledge very difficult into the law curriculum.

The slowness of legal developments and adaptations can take a very long time. As one legal expert put it, "*This kind of technological revolution, if you want to call it that, just takes forever in the legal world.*" (I-9) The legal system develops slowly. This can lead to gaps in the law that make the practical work of legal experts very difficult. The traditional structure of the legal sector makes it difficult to integrate new technological developments into the legal landscape. This can cause the legal world to lag behind the technological developments.

But the speed of law versus the speed of technology is not the only hurdle. There is also the challenge of creating legal frameworks for technologies. As discussed earlier, legal vagueness allows the law to develop along with technological developments, but it also leads to a lack of clarity that can hinder the work of legal experts in assessing Privacy-Enhancing Technologies. There is a need to find more ways to bring these worlds together.

6.3. Organizational

In addition to regulatory and technical-legal hurdles, organizations face organizational challenges in implementing PETs. These challenges range from a lack of resources to cultural barriers in data protection to special requirements for small and medium-sized enterprises that may not have the same resources or expertise as larger organizations.

Challenges	Mentions	Interviewees
Lack of resources	(I-3), (I-5), (I-6), (I-7)	4
Late involvement of legal experts	(I-1), (I-2), (I-5), (I-6), (I-8), (I-14), (I-15)	7
Demanding collaboration with regulators	(I-1), (I-4), (I-5), (I-3), (I-6), (I-8), (I-10), (I-11)	8
Particular challenges for small- and medium-sized companies	(I-1), (I-2), (I-5), (I-7), (I-8), (I-11), (I-12)	7

Table 6.3.: Organizational Challenges

6.3.1. Lack of Resources

One of the challenges for legal practitioners in supporting the use of PETs is the lack of resources. There is an awareness of the need for technical measures, but often not the resources to support their use. This limitation can hinder the process of adopting PETs. Streamlined processes and organizational structures must be in place for successful implementation and ongoing monitoring. The need for increased collaboration and process optimization is constrained by resource allocation.

So, it would be good if somewhere the processes could be made a little more efficient in that sense, there is a continuous exchange.

> That would not be harmful. No, not harmful, I don't know. But not really feasible? It is feasible, but the question is with what resources, and continuous is such a nice word, regular. So of course, we have a continuous improvement process there. The question is, what does discontinuous mean? (I-11)

This interviewee also brought the point up, that an organization must find the right resource allocation. This must be profitable for an organization. Often there is still the problem that organizations see data privacy as a marginal topic which can lead to a lack of investment in this sector. On top of that, there is often a negative association with data privacy compliance within organizations: "*The perception is likely to be that it slows down development. And that it always costs a lot of money.*" (I-6) There is a need to create more incentives to invest in the implementation of Privacy-Enhancing Technologies.

Another aspect is the cost of time. The selection, evaluation, and implementation of a PET is not just about choosing a solution. For legal professionals, it involves understanding the technology and ensuring data privacy compliance. This process takes time, which many organizations cannot find, as mentioned. "*The time to do this is, of course, the other obstacle to bringing advanced products to market.*" (I-1)

Furthermore, the implementation of Privacy-Enhancing Technologies can be costly. From a legal perspective, this factor must also be considered. When choosing technical measures, the cost of implementation is an aspect that has to be considered due to Article 25 [7].

> Because sometimes the legal departments are also involved in data protection, depending on the company, it is simply too thinly staffed and is then dependent on external advice, i.e. external counsels. That means there must be a budget for that. That leads to budget problems, which delays the whole thing again because the cost of the advice can be immense. And that sometimes slows down a product like this. (I-6)

Lastly, the adds to these challenges. There is a need for legal experts with technical background or knowledge. It is mentioned, "*It's better to have a lawyer with technical knowledge, but there aren't that many. It's also very difficult to find capable people in this area that you don't train yourself.*" (I-5)

6.3.2. Too Late Involvement of Legal Experts

When legal experts come late to the process of implementing and using Privacy-Enhancing Technologies, the problems between technical solutions and legal requirements become even more difficult to manage.

> At what point is the lawyer really relevant? Very early, in my opinion. Right from the conceptual phase. (I-1)

> It is a big problem that the project is developed and then legal advice is sought somewhere. (I-2)

At the beginning of the development of a new product, the technical requirements for the system are defined. At this stage, legal experts are often not involved. This has the consequence that legal experts cannot inform and educate their technical colleagues about the legal requirements to ensure data privacy compliance. Also, Privacy-Enhancing Technologies should be considered in the design phase of a product which is often done because of legal advice. In addition, legal experts are not able to understand the product in advance. Therefore, they cannot give special legal advocates to their technical colleagues.

> You either get out of the way or you understand it yourself and then say early on that at this point you need to be careful about what you take, why you take it, and how you take it. (I-2)

The late involvement of legal experts can lead to many problems. On the one hand, it is often difficult to implement privacy-friendly technologies after the fact instead of building them into the system from the beginning. On the other hand, this can also lead to high costs.

> I don't know about your experience, but if you tell the software developers a week before going live that this solution is not compliant, everyone is not very happy. (I-11)

One possible reason for this delay in seeking legal advice is the often low level of privacy awareness in organizations. If departments were more educated about privacy requirements, they would seek legal advice more often. Similarly, technical departments are often only aware of IT security but lack knowledge in data protection and its technical requirements. Legal professionals are also often seen as an obstacle:

> They don't want a lawyer to explain the law to them, they don't care. So that's the way it is, They don't sit there and say it's exciting, we're here today, it's about privacy, they say this is the product, this is how it has to be, we have to make it work so it works. (I-6)

Privacy awareness is beginning to grow, but it is still in the early stages of change.

> It's not automatic to bring in privacy lawyers and keep an eye on it, I'd rather say we're not there yet. But the awareness is there! (I-6)

6.3.3. Demanding Cooperation with Regulators

The field of data protection and Privacy-Enhancing Technologies is still evolving. Its dynamics require close cooperation between organizations and regulators. Ensuring the proper implementation of Privacy-Enhancing Technologies is a challenging task. Mainly because there is a lack of legal frameworks and specific guidance on the use of PETs. One interviewee describes this challenge in more detail:

> And they are very careful with what they say anyway, so they say that we are not giving any concrete guidance, but we will look afterward to see whether it was right or wrong, whether it was sufficient for us or not, because of course they always see the risk if they somehow say that it is sufficient and then something happens or someone uses it incorrectly or depending on the situation, that there will always be a risk that it is not sufficient for us, that then always the supervisory authority has to represent it. And of course, they don't want that either. That's why they keep a very low profile on all controversial issues or are very strict, depending on the issue, so strict that it can't be implemented in practice. Unfortunately, that's how it works in practice. So supervisory authorities, already issue things, for simple cases, but for really such borderline cases, unfortunately, there is simply little. (I-5)

The dilemma is obvious. Regulators have the difficult task of ensuring that PETs help to achieve data privacy compliance. At the same time, they want to support innovation. In this

evolving field it is a huge challenge for regulators to standardize and regulate the usage of PETs.

The resulting lack of guidance creates many difficulties for legal professionals when it comes to supporting the use of Privacy-Enhancing Technologies for data privacy compliance. The unclear legal landscape hinders legal experts from evaluating Privacy-Enhancing Technologies legally.

> Regulators usually tell you what not to do. But they don't tell you how to do it. (I-8)

Boundaries are set, but no clear guidance within these boundaries. As a result, organizations are often uncertain when it comes to Privacy-Enhancing Technologies. They do not know how to find a balance between innovation and compliance. Ultimately, the nature of legal professionals is that they often choose a path of certainty and security which leads to an avoidance of Privacy-Enhancing Technologies. As a result, some legal professionals are very frustrated with the lack of guidance from regulators:

> What bothers me the most, personally, is that you're left a little bit alone by the regulators. That's really the biggest criticism. (I-11)

Lastly, the cooperation with regulators is even more difficult due to their dual role. They do not only give advice or recommendations. They are also the bodies that impose penalties for non-compliance. This can discourage legal professionals from seeking clarification from regulators as they fear of being targeted and potentially punished.

6.3.4. Limited Expertise in Small- and Medium-Sized Organizations

The implementation of Privacy-Enhancing Technologies for data protection compliance poses unique challenges for small- and medium-sized enterprises (SMEs). Legal experts often face huge challenges in supporting the use of Privacy-Enhancing Technologies at small and medium-sized organizations due to their limited resources. This applies not only to financial resources but also to human resources.

> They don't call me up and say, "Hey, can I get legal advice for 200 euros an hour?" Okay, that's actually more possible if you're maybe in a big company where there's an in-house legal department, but you definitely have to do that again. (I-2)

Unlike multinationals, SMEs do not always have the luxury of having separate legal, IT, or privacy departments or teams. As a result, the roles are combined, requiring employees to juggle multiple responsibilities.

> The biggest challenge, especially in smaller companies, is the workload. It's rare that one person is completely responsible for privacy, but it's 30 percent of their workload. Soon it will be 150 percent, and that's difficult. That's where I see the biggest problems. (I-5)

The sheer burden of managing, understanding, and implementing Privacy-Enhancing Technologies often falls on existing legal professionals, who are not always specialized in privacy law.

> So, first of all, the staff. We need people who can evaluate it and who can implement it in the first place. That's where it really goes wrong. (I-7)

In addition, many Privacy-Enhancing Technologies are still in the early stages of research and development [9]. Therefore, they can be still very complex and difficult to implement [9]. Accessing and integrating these technologies requires not only expertise but also significant technical resources. This is often not achievable by SMEs.

> Small- and medium-sized enterprises, have a very hard time there. [...] and things like Homomorphic Encryption, where it's still in the research stage, I would say the resources required are way too high, and that's what the big Silicon Valley companies are doing, but otherwise only the big ones. (I-7)

7. Solution Strategies and Concepts

To answer research question three, this chapter examines solution strategies that address the challenges identified in Chapter 6. These findings are based on the interviews and further insights from the literature. During this research, additional literature was found as a result of insights from the interviews and can be found in Appendix C. At the beginning of the chapter, a table presents the overall solution strategies and the total number of the interviews in which they were mentioned. The solutions are divided into six groups. Each solution strategy, except the first one, is divided into sub-solutions. Each group is presented with a table showing the interviews in which it occurred and the total number of mentions.

Solution	**Mentions**
Interdisciplinary research and collaboration	6
Increasing awareness	6
Standardizing data privacy compliance	12
Fostering collaboration of technical and legal experts	9
Improving education	13
Enhancing guidance	15

Table 7.1.: Solutions Overview

7.1. Interdisciplinary Research and Collaboration

Solution	**Interviewees**	**Mentions**
Interdisciplinary research and collaboration	(I-1), (I-3), (I-4), (I-7), (I-11), (I-12)	6

Table 7.2.: Interdisciplinary Research and Collaboration

Some Privacy-Enhancing Technologies are still in development, while others are already in use for data privacy compliance. Legal experts must ensure the reliability of a product when assessing its suitability for data privacy compliance and many PETs are not ready for the market and need to be further developed between different disciplines.

There is a need for joint research and dialogue between legal experts and PET manufacturers. As one senior interviewee who works closely with the industry put it:

> We're not there yet, but where are we going? The question is, where are we going with PETs? Let's say we have them. What does privacy need now? (I-3)

Involving legal experts in the development and research of PETs can help ensure that these tools reach their full potential for privacy compliance. This collaboration can significantly narrow the gap between technology and law by ensuring that these technologies can meet legal requirements. In addition, improved communication with Privacy-Enhancing Technology suppliers, comprehensive documentation, and expert discussions can foster trust and mutual understanding. One respondent talked about their law firm's close collaboration with technology companies: "*We have very close contact with them.*" (I-3) He mentioned that he often has "*expert discussions*" (I-3) with developers to understand in more detail how the technologies work and how they can be used for data protection compliance. A good working relationship between PET suppliers and legal experts can enhance their expertise and ability to support the use of PETs.

The involvement of legal experts in legislative processes can also help to develop the legal landscape for PETs. One respondent mentioned that this often takes the form of "*traditional association work*" (I-8). In this context, legal experts can represent the needs of legal practitioners for the use of PETs for data protection compliance. This collaboration can improve the legal landscape with respect to Privacy by Design and PETs by clarifying legal concepts or articles such as Article 25. The practical insights of legal experts can help shape laws and regulations in a more practical direction.

Collaboration with academia also plays an important role in bringing more clarity to the legal applicability of PETs. Collaboration between legal experts and academics can help both sides. This partnership fills research gaps and provides legal experts with the latest technical knowledge to support their arguments. At the same time, legal expertise guides research on the practical application of PETs within the legal framework. This exchange promotes solutions that reconcile PETs with legal requirements. This can help build a solid foundation for effective privacy practice by legal professionals:

> Of course, it is also important for us externally, for example, to cooperate with academia and to do some academic work ourselves in some areas, especially when it comes to new technologies or when we are dealing with public authorities. (I-8)

In one interview, a legal expert particularly emphasizes the need for interdisciplinary research. Data privacy compliance must consider not only technical and legal aspects. It also needs to be aligned with internal resources, structures, and use cases. Therefore, interdisciplinary research on PETs can help legal experts assess PETs from a holistic perspective, which can help evaluate their use for the organization. This is emphasized by one interviewee:

> Ideally, we need to really cross disciplines, really cross fields of study that you can get, that you get business information scientists involved, that you get lawyers involved, that you get economists involved, that you get statisticians involved, [...]. Because all these topics have suffered from the fact that there have been technicians who have said, yes, that's possible, that's totally good, but there's also a myriad of very complicated, yes, cryptological methods that are used [...], and that's where all the enthusiasm and just jumps off. And when it comes to saying where the economic added value is in terms of business administration and economic value of this kind, so that they can go, then you need people's values for that, and you need reliable figures, and we can't give them that now, so they jump off very quickly. (I-4)

Looking at the literature, the Royal Society report also emphasizes the need for interdisciplinary research to provide more clarity on the applicability of PETs, which is essential for their legal assessment [22]. The report calls for more support from science funders. They should invest in challenges, projects, and international test beds. Governmental and intergovernmental bodies can also provide a framework for the practical application and understanding of PETs. The report also calls for the promotion of partnerships between researchers, universities, and the private sector. When there is consistent practice and understanding, regulatory assessments are easier to make. The private sector can also provide real-world contexts. Bodies such as the United Nations can also provide test environments. These sandboxes allow the practical testing of PETs. This can provide scenarios for legal experts to evaluate and understand. The Royal Society also calls for research into the societal and economic impacts of PETs. Legal experts can use this broader perspective on PETs to make arguments [22].

7.2. Increasing Awareness

Solution	Interviewees	Mentions
Organizations	(I-4), (I-6), (I-8), (I-14)	4
Public	(I-1), (I-8), (I-9), (I-14)	3

Table 7.3.: Increasing Awareness

7.2.1. Organizations

Creating a robust culture of privacy within organizations is a key strategy for improving legal compliance with Privacy-Enhancing Technologies. Legal experts can function as a voice for data privacy and educate on its importance. In the interviews it became clear that the GDPR had increased the awareness of privacy significantly, but that there is always the need for ongoing communication and clarification:

> The requirements, for example, the GDPR requirements, lead to the fact that people look at privacy. You must talk to people; you have to really engage in the discussion and keep explaining that this is not an end in itself. (I-8)

Creating a data privacy culture at the organization is the prerequisite to support legal experts in the process of data privacy compliance when PETs are used. The specific departments must involve the data privacy compliance teams. If there is a positive organizational culture toward data privacy compliance, legal experts are often more involved in the processes of the specific departments. In the end "*the real linchpin, then, is raising awareness of the need for such measures. The whole thing stands or falls on that.*" (I-8)

While fostering a strong culture is critical, care must also be taken not to hinder business operations. As one interviewee states, "*You can't stifle people either, but people have to, colleagues have to do business or something, now again from the company's point of view, they have to keep the company going, no matter what area we're in.*" (I-8) This balancing act is also further described in the danger of over-caution and scaring colleagues with the topic of data privacy compliance:

> So, the other extreme would be if the colleagues were to go into such a state of shock that nothing happened at all. That would be unfortunate. And to find the right measure there, I think that is to the, the very, very greatest challenges between those. (I-8)

To create a data privacy culture at an organization it is important that data privacy compliance and Privacy-Enhancing Technologies are not seen as organizational obstacles, as it is mentioned:

> So, I think, quite centrally now, also in comparison to the activity at the university, my activity is really an enabler. In the best sense of the word, we try to create a convergence between data protection requirements and the people behind them, which is what it's really all about, economically driven necessities. (I-8)

It is necessary that legal experts also see the economic side of data privacy compliance. To create a data privacy culture, organizations should not be threatened by data privacy compliance. If legal experts are recognized as enablers, and not as restrictors, they are more likely more involved which makes the process of data privacy compliance much easier. They have to build a cooperative climate:

> In the beginning, it's natural, especially when you're working with colleagues for the first time, then of course it already feels a bit like the cut or the limitation of creativity. [...] I believe that we have now created a really good working relationship with 90 percent of our colleagues from the development areas, where we are perceived as colleagues who really support this, and who do not somehow try to artificially emphasize restrictions or make data protection more important than it is. (I-11)

Increasing awareness is still in the learning phase. It must be further strengthened through constant learning and repetition. This can be achieved by training, "*But yes, it is a learning process. We also do an incredible amount of training. At least once a month, we have two to three hours of training where we go over things in detail.*" (I-8) These trainings and open dialogues with colleagues can help to create a data privacy culture at organizations.

Available literature suggests that promoting awareness of Privacy-Enhancing Technologies in organizations has several benefits. ENISA research [50] suggests that privacy features are overlooked in traditional technical approaches, primarily due to limited awareness and understanding by developers. To increase the adoption of Privacy-Enhancing Technologies, organizations need to strengthen the awareness of Privacy by Design in technical departments. Legal experts can use their knowledge of the legal framework to close this gap and encourage companies to develop systems and services that inherently prioritize privacy. The shift by policymakers to view privacy as a benefit rather than a cost is fundamentally changing the perception of Privacy-Enhancing Technologies in organizations. Legal professionals can help in this process by promoting Privacy-Enhancing Technologies not just as compliance tools, but as strategic assets that add value to the business. When privacy becomes a benefit, the motivation to integrate Privacy-Enhancing Technologies is naturally greater [50].

The Royal Society report [22] recommends integrating Privacy-Enhancing Technologies into training and certification. This is a strategic step toward creating a culture of privacy awareness from the ground up. Legal experts benefit in several ways. They have a better-informed audience, but they also have in-house professionals with a basic knowledge of Privacy-Enhancing Technologies. This makes implementing and managing these technologies much easier [22].

7.2.2. Public

Public awareness of privacy helps to promote the importance of technical measures, such as Privacy-Enhancing Technologies. This also helps legal experts in reinforcing data privacy compliance. With increased public awareness about the value of data and its potential threats related to it, people become more knowledgeable about their rights as data subjects. This is also where awareness must be generated:

> It is important to make the people concerned really understand in such a way that they understand that their data has value, that it is nothing more than the five-euro bill in their wallet. (I-8)

A better-informed public is more likely to demand transparency from companies. This increased demand forces companies to be more open about their data practices and even can make data privacy a competitive advantage for organizations. This way, organizations will more likely adopt Privacy by Design and thereby also PETs. One interviewee suggests that discussions and debates on laws around data protection can be shaped and further developed:

> Yes, especially if you demand laws, it is actually also essential that society deals with it, because a lot happens through discussion and dispute, and if ultimately no one is interested or if no one understands, then there are also few people who demand it, and then it happens slowly. (I-9)

This emphasizes again that public awareness increases the motivation of organizations to invest in more technical measures for data privacy compliance. This can be beneficial, especially for complex technologies like PETs. A legal expert also mentioned that these technologies can easily help to show the efforts that a company has made in data privacy compliance:

> When we implement privacy management systems, this aspect of Privacy by Design and Privacy by Default plays a big role because that's, let's say, one of the most thankful stories you can do upfront as prevention. (I-4)

In literature the Royal Society [22] emphasizes that governments should be role models in adopting PETs and advocate for their usage, especially in public-private partnerships. By leading such initiatives, governments can foster trust. Demonstrating the practical application of PETs, especially through proof of concept and pilot projects, educates the public on their value. Such demonstrations build trust and highlight the importance of PETs in various sectors, like healthcare, research, and public data use. For legal experts, such demonstrations serve as evidence when advocating for PET's implementation [22].

7.3. Standardizing Data Privacy Compliance

Solution	**Interviewees**	**Mentions**
Processes	(I-1) (I-2), (I-4), (I-6), (I-7), (I-8), (I-10), (I-11), (I-13)	9
Audits	(I-4), (I-5), (I-7)	3
Certification	(I-2), (I-3), (I-5), (I-6), (I-7), (I-8), (I-10), (I.11), (I-12), (I-14)	10
Tools	(I-1) (I-2), (I-3), (I-4), (I-5), (I-7), (I-11), (I-14)	8

Table 7.4.: Standardizing Data Privacy Compliance

7.3.1. Processes

The ability of legal professionals to support the use of Privacy-Enhancing Technologies can be greatly enhanced by standardizing privacy compliance across an organization. Legal

professionals can help establish a structured framework.

Data Protection Management

Under the GDPR, organizations must be able to demonstrate how they comply with the legal requirements for data protection. This is referred to as the "accountability obligation" in Article 5 [7]. This is where a data protection management system comes in. It helps to ensure that all GDPR obligations are met in an organized manner. Therefore, legal experts must take on the role of managing data and ensure that a framework supports the data protection compliance process, especially when using Privacy-Enhancing Technologies. Legal professionals advise organizations on data management:

> I teach companies to be responsible and aware of data, and you do that by addressing the issue, and it's almost like any other compliance issue, ultimately with an appropriate management system, whether it's an information security management system or a text compliance management system or whatever, it's always the same thing, you're trying to implement the regulatory or legal requirements as effectively and efficiently as possible. (I-4)

Finally, there are document systems that sit behind the organizational structures. One legal expert explains how to build a data management system:

> By management system, I mean document systems that are behind data protection, that is, many need to build a coherent system, which therefore designs a data protection policy, which builds all the basic documentation. And all of that, as a self-contained document system, is then called a management system. And it's best to build it in a modular way so that it can be linked together. Level 1 is called the privacy policy. [...] A policy is always a foundational document that describes the requirements that a company must meet in terms of privacy. We follow the principles of Privacy by Design, Privacy by Default, and so on. (I-10)

Privacy By Design can be included in the requirements of the privacy policy. Legal experts can include the requirement to use technical measures such as Privacy-Enhancing Technologies. The second level of a data management system is to build the respective processes. These can help to achieve an efficient data privacy compliance process with PETs:

> For example, you can develop a core process that says, when we launch new products, we're going to meet this requirement so and so. (I-10)

> It is about designing the organizational structures so that the processes can run properly and as efficiently as possible. (I-4)

In complying with PETs, another important part of the process is the cooperation between the technical and legal departments from the very beginning.

> Timely involvement is a top priority for legal professionals. We have processes and policies in place so it's clear who's responsible for what and what the processes are, which makes it easier. (I-5)

As mentioned earlier, communication channels should also be established between other roles and functions:

> If you're going to launch a new product, it's important to involve all departments in the development of the product or service. And that's where you can anchor all these issues. You can say, okay, if your new product is going to be built, then by default the following requirements apply. That is, it has to be built so that it's clean right from the start. (I-10)

A good way to build privacy into process development is to create gates. Such gates ensure that no product is completed without legal advice on Privacy-Enhancing Technologies. This can help integrate legal requirements into technical requirements and the design phase:

> We place great emphasis on mapping the relevant requirements in new developments. We now have real gates in our development processes where we say that privacy is now an issue, especially in products where we use cameras, for example, where we simply say this is a gate and if there is no privacy check mark on it, then the output will not be released. (I-11)

Ultimately, structures and processes are the foundation for a successful and efficient data privacy compliance process with PETs.

Using Synergies With IT-Security

IT security and legal departments often face the same challenges. Their approaches should be more aligned. When trust grows, it leads to more effective collaboration. This unity can simplify the implementation of Privacy-Enhancing Technologies. It makes the organizational adoption of PETs easier and more compelling. For example, certain PETs can simultaneously ensure data anonymity to meet legal requirements and at the same time act as a data breach protection mechanism, which benefits IT security goals. One respondent elaborated on the idea of combining IT security and privacy processes:

> As a privacy officer, I can't just bring in any IT security policy; the IT security policy has to come from the IT department. Of course, it may be possible or useful to start with that or to introduce data protection aspects right away, i.e. to say that the following data protection principles must be observed when creating an authorization concept and, depending on the company, if I do it at the company level, to say right away what the data protection situation is in the individual company. I can also summarize this more generally and say that, in principle, the privacy policy should look like this and go through the individual areas, IT

> security, and so on, and then it should be implemented immediately. So it's not a bad idea to say right away that it always has to be taken into account, because otherwise I come to the point that we often have, where a system or a concept or something else is introduced and then it has to put on the brakes and the whole thing has to be changed again. (I-5)

> We hear that from our ISO colleagues all the time. And they say, hey, we're actually in the same boat. And if you need an encryption measure, and we need an encryption measure, let's work together. (I-8)

By combining the strengths of the legal and IT-security departments, organizations can incorporate privacy considerations at the outset of security initiatives. By emphasizing the importance of PETs to IT security managers, their adoption rate could increase.

7.3.2. Audits

Regular audits for Privacy-Enhancing Technologies can further mitigate the risks associated with their implementation. Audits assess not only the effectiveness of such technologies but also their compliance with privacy principles. Audits naturally require cooperation between legal and technical experts. This regular interaction promotes mutual understanding and bridges potential communication gaps. As a result, legal professionals do not need to be IT experts to evaluate IT initiatives, confirm their feasibility, and ensure that they comply with the regulatory framework:

> And of course, you now know a lot more about information security. You don't have to do it all yourself, but you do have to do the audits, in the other departments or specialties to be able to evaluate the audits, What you are doing sounds good and plausible. I'm going to check it off now. (I-7)

Audits enable legal professionals to ensure compliance while improving their technical expertise. This helps further to bridge the gap between technical and legal knowledge.

Compliance is an organizational challenge that naturally requires cross-functional collaboration. Audits provide insight into specific departments to ensure that privacy measures are consistently implemented across the board. Legal professionals can use these audits to provide oversight of the technical area and promote a cross-functional approach:

> Yes, so it has to be interdisciplinary. That's what I was alluding to a little bit with these audits, so privacy officers with a legal background don't have to be information security experts but at least they have to do audits. At least, that's my opinion, they need to do audits in the area of information security and then use those audits to take control in that area. But they do not have to be experts themselves. So that's another way to close the gap a little bit. (I-7)

7.3.3. Certifications

As discussed, there is a vague legal and regulatory landscape for Privacy-Enhancing Technologies. Legal experts need additional sources to bridge the gap between the technologies and the law. So standards and certifications, as often mentioned, are needed:

> Definitely. The need is 100 % there. The legal requirements are very high, but the requirements are so high that it is hardly possible to develop the corresponding requirements for the certification program. (I-6)

Although there is a great need for standards and certification, there are still several obstacles in the way, which became clear during the interviews:

> The regulator always says that you, the industry, make the industry standards. But in practice, this is still a long way off. (I-3)

There are several steps that need to be taken to create standards and certifications. In the GDPR articles:

> That's an example, which is also still the question of how it comes and how it works. So Article 42 certifications. So that would be exactly what you would always hope that there would be certifications at some point. But it is just not there yet. So these are articles that need improvement, which is also very much lacking. (I-5)

> We have now, today, we have for the first time, had the regulatory committee a few weeks ago for the first time decided the criteria for the certification institutes, which then around that they accept the certification procedure. So, yes, I need someone to develop a standard, and then I need someone to certify that standard. Now there are criteria for these certifiers. So, I don't have a certifier yet, and I don't have anyone who has developed a standard. (I-3)

Standards and certification help legal experts in the process of data privacy compliance with PETs. They help to fill in the gaps in regulations and laws and can give legal professionals confidence in these technologies. Furthermore, they provide proof of compliance and of what is being used in the marketplace. However, the state-of-the-art required by the GDPR refers to industry standards, and they do not exist yet:

> That's why we are always very concerned, or we have to be very concerned, about what is available on the market and also suitable for this problem. (I-12)

Standards and certifications provide legal professionals with a structured and widely accepted framework for understanding and advocating the use of Privacy-Enhancing Technologies. They can provide a clear roadmap for compliance and ensure that technologies are compliant. They serve as a common language, facilitating communication between technical and legal

experts. By adhering to recognized standards, legal professionals can lead organizations with confidence, knowing that these technologies meet specific criteria and comply with both industry best practices and regulatory requirements. Standards and certifications reinforce the trust, clarity, and credibility that legal professionals need when incorporating privacy technologies into their compliance strategies.

The literature also provides some insight into standards. The ICO report [9] on PETs emphasizes the importance of practicality when adopting PETs and advises organizations to rely on established standards to defend against threats and technical measures. The Royal Society [22] suggests that a reliable certification scheme for PETs will increase business confidence in data sharing and processing. They also advocate the adoption of Privacy Enhancing Technology protocols and standards by prominent standards development organizations. They emphasize the adoption of open standards to drive the growth of PETs and ensure their reliable implementation in data management. Organizations such as the British Standards Institute (BSI) and the National Institute of Standards and Technology (NIST) should lead the effort, building on existing cryptography standards [22].

7.3.4. Tools

The term "privacy tools" refers in this context to technologies that can support the work of legal experts through atomization and artificial intelligence. It was clear from the interviews that this process is just at the beginning and that there will be a massive change in legal practice in the future. In one interview, it is mentioned that it would be helpful to have a tool that can give feedback on pseudonymized or anonymized data:

> They just need software that they can just run the data through. In the end, they get something that is privacy-compliant. That's what I would say small and medium businesses need. But it's still a whole problem. You are now pseudonymous or anonymous. This is what the standard user needs at the end. (I-7)

The literature review also showed that there are many attempts to analyze regulatory requirements in a logical way. Tools such as Alloy, a specification language for expressing structural constraints, have been used [29].

The legal tech sector has grown continuously in recent years [51]. In 2022, the size of the legal technology market will be $23.45 billion. By 2030, according to a new report from Grand View Research, it is estimated to reach $45 billion [52]. In one interview, this evolution is discussed, there will be a shift to atomization and artificial intelligence:

> So if we're talking specifically about law and technology now, I would argue that in a few years, we're going to see a significant change, we're going to have a very different landscape in this area due to the emergence of legal tech. (I-10)

> So I would say that the whole law firm landscape is going to be mega disrupted and lawyers are going to increasingly become highly specialized experts or disappear. (I-10)

This quote underscores the need for legal professionals to follow the latest technological developments in order to stay relevant. This means being informed about PETs and being able to work with privacy tools. These technologies could have tremendous benefits for the data privacy compliance process, especially in terms of cost reduction and time savings. However, Privacy-Enhancing Technologies often fail because of the costs associated with their implementation, but also because of legal advocacy:

> It is also often pleasant for the legal experts. [...] They have more time for the really exciting things and not for this 'small stuff'. (I-2)

> Especially if you look at the hourly rates, the lawyers, the interest of the clients is very high to replace them as much as possible. That is, any form of technology that minimizes legal work is bueno. In any case, a good thing. (I-2)

The use of tools can improve the ability of legal professionals to support the use of Privacy-Enhancing Technologies. But there are still some challenges related to newly developed technologies, such as their maturity and limitations:

> It can analyze and aggregate information much better than we can.[...] But then the interaction, the evaluation, and if there is a certain state-of-the-art. The machine will not be able to do that. (I-3)

> Where it's simply not that simple, where it simply depends on human input, on legal evaluation, which is not always black and white. (I-5)

7.4. Fostering Collaboration between Technical and Legal Experts

Solution	**Interviewees**	**Mentions**
Cross-functional teams	(I-1), (I-2), (I-3), (I-8), (I.11), (I-13), (I-15)	7
Cross-functional training	(I-6), (I-7), (I-8), (I.11), (I-13)	5
Supporting tools	(I-1), (I-2), (I-3), (I-6), (I-7), (I-8), (I-11), (I-15)	8

Table 7.5.: Fostering Collaboration between Technical and Legal Experts

7.4.1. Cross-Functional Teams

Fostering effective collaboration between technical and legal experts is essential to support the ability of legal experts to support the data privacy compliance process with PETs. Building cross-functional teams from the beginning allows the early involvement of legal experts.

The technical and legal departments are the two main actors in the data privacy compliance process. It is essential that there are clear channels of communication. As legal professionals rely on the technical expertise of their colleagues, clearly defined roles and responsibilities are essential, especially when selecting and evaluating Privacy-Enhancing Technologies for new products. The creation of cross-functional teams can help tremendously with the usage of PETs in the privacy compliance process:

> I'm in direct communication with the information security department, and I often say, "Okay, we have some new software that's going to be deployed, for example, the technical organizational measures. Have you guys reviewed it? Do you want us to review it? Are we reviewing it together? Are we coordinating on that?" (I-8)

> We also write what we call process specifications and things like that ourselves, but we really write them in a way that we don't want to get in the way somehow, but our goal is always to get involved in things like that as early as possible. Get us involved as early as possible, get us on the project teams, and then we'll help you in that way. (I-8)

> Trust, a good working relationship, and that we get a standing so that we are there at the kick-offs when new projects, pre-developments, etc. are started. (I-11)

Misunderstandings and communication barriers can be the greatest obstacles to the implementation of PETs. This interdisciplinary approach also guarantees that the best solutions will be found. Sitting around a table and discussing a new project is the most effective way to bring technology and law together. "*So I also had workshops with the colleagues who are in the house, the lawyer and the whole department.... 10, 15 engineers and explain to me, completely, how it works, we learn it together.*" (I-6) By learning together, teams not only acquire the knowledge needed for a project, but also build trust and understanding among members, which leads to better communication.

Open dialogue is the foundation of an effective collaboration. "*And then, thank God, I have great colleagues who explain it to me, try to explain it to me, and then I can evaluate it.*" (I-8) The willingness to ask questions, seek clarity, and persist in seeking understanding is critical. "*But then, in order for me to make a statement, we just keep asking until I understand it, as much as I need to understand it.*" (I-6)

It is crucial to understand and respect the limits of each other's expertise: "*I think that's just not possible today because the complexity has increased.... I think it's hard to be an expert on everything.*" (I-11) This statement underscores an important insight, no one person can be an

expert in everything. That is why the value of cross-functional teams is becoming increasingly important. Rather than expecting legal experts to be IT security experts, or vice versa, the solution is to leverage the collective strengths and expertise of a diverse team. In this way, organizations can ensure that the knowledge required for complex projects is represented.

7.4.2. Cross-Functional Training

Cross-functional teams ensure diverse expertise and communication from the start.This collaboration can be further fostered through cross-functional training on their topics, as one interviewee put it, "*What we are already doing is with the two colleagues who are consulting with me in this area. We have training in the areas, in both directions. So, of course, we train the areas legally, but they also train us in the other direction.*" (I-11) This mutual learning is an essential component of these teams and fosters an environment where both the legal and technical experts increase their understanding for eachother.

It is also interesting to note that a deeper technical knowledge can, of course, be very useful and effective in working with technical colleagues. This can improve the quality of legal advice, as one expert put it:

> I really think that the closer you get to the technical side, the better advice you can give because it really comes down to the details and really understanding both the purpose of whatever the technology is and how it works so that you can have that conversation, that brainstorming, that offering suggestions that are valuable. (I-15)

It must be said that this interview was conducted in America, where there are far fewer laws and regulations in place. In Europe, it was also the case that everyone agreed that more technical knowledge is beneficial, but it must also be feasible, as discussed earlier.

In terms of cross-functional training, it is important to mention that both sides need to be trained to make the privacy compliance process more efficient. Also, training the technical side is very important to better support Privacy-Enhancing Technologies. In addition, technical teams should have a basic knowledge of privacy laws. As it is stated, "*Yes, for the most part, I think it's now essential for software developers to have a basic knowledge of privacy law*" (I-11). Training that focuses on basic legal requirements, such as Articles 25, 32, and 35, can provide technical teams with a basic legal knowledge of Privacy by Design. One interviewee referrs to this training as "*my package that I always go through.*" (I-7)

One interviewee emphasizes, "*It's important for lawyers to maintain that basic acumen for technology.*" (I-13) But this goes both ways. Technicians should also be familiar with international security standards, and guidelines from standards organizations. In essence, "*both teams need to have a minimum understanding of each other's function*" (I-15) to foster collaboration and ensure effective problem-solving in a world where technology and law are increasingly intertwined:

> So, I will then educate my technical team about this regulation. Then my technical team will procure that technology, and they will build that technology, and then we will talk to each other. (I-13)

7.4.3. Supporting Tools

Cross-functional teams and cross-training are the foundation of good collaboration between technical and legal departments. As often discussed, legal and technical experts need to find a common language. Supporting tools can help achieve this goal.

Visualization

A recurring theme in the interviews was the need for visualization in the communication between technical and legal experts. It is a huge challenge for legal experts to understand all the processing activities of a new product. Several interviewees mention the need for visualization, for example in the form of data flow charts:

> So really, I always have that, I really love data flow diagrams. Then I say, okay, draw that for me, dear IT people, so I can understand that. And then I don't really care what the system is called and how it works in the background, as long as I understand how the data processing works. (I-8)

Visualization can act as a translation tool between legal requirements and technical implementations. A very interesting approach was found in the paper "A model-based framework for simplified collaboration of legal and software experts in Data protection assessment" [53]. They propose a framework to facilitate communication between legal experts and software architects. They also refer to data flow diagrams, which can describe and analyze software architecture. They can represent the flow and processing of data in a system. The model would be two-sided. It suggests a structural model for the software architecture and a structural model for the legal requirements[53].

Glossary of Terms

The interviews revealed that there are several "language barriers" between legal and technical experts. Although legal experts rely on technical experts to confirm the accuracy of technical terms, it is essential that both understand the implications of definitions in each other's domain [10]. There is a need to build a common privacy vocabulary between users, lawmakers, and IT developers [11]:

> Yes, it would be cool if somehow the lawyer writes to somebody who has a technical understanding of it, because the lawyer knows the terms of the GDPR, knows what it means to collect, and knows what it means to process. But if somebody then says yes, at this point, it goes into this form, it goes into the backend, it writes it into the database. [..] What happens there? So it would be quite good if both worlds could come together at this point. (I-2)

Navigating data privacy requires skillful communication between technical and legal experts. One promising strategy is to create a common glossary. This would act as a bridge, translating technical jargon into legal language and vice versa, thereby simplifying and improving collaboration.

This would promote consistent communication, reduce misunderstandings, and potentially serve as an educational tool for both parties. However, there are also challenges to consider.

There is a related work in the literature: "Law for Computer Scientists and Other Folks" that introduces law and its definitions to computer scientists [54]. The book covers various topics such as privacy, data protection law, and cybercrime. The book is not intended to turn computer scientists into lawyers, but rather to show how law and the rule of law protect privacy, for example, and how this is relevant to computer scientists [54].

Checklist

> I think it's good to create such a checklist, because privacy law already works with checklists, and these basic templates are already quite applicable. As I said, small modifications for the specific use case, but very plausible. (I-2)

As I explored the use of Privacy-Enhancing Technologies for privacy compliance, it became clear that checklists are a proven tool for data privacy compliance. These checklists are useful for getting the technical and legal teams to work together, especially as a starting point for a new project with PETs:

> There is no such thing as a 100 %checklist that you can go through and be done with it. (I-7)

However, creating checklists for PETs presents several challenges. There are not many guidelines for PETs, and there is a lack of practical experience with them. More research is needed on what these checklists could look like. They should show how PETs fit in with data protection laws and include details specific to the technology. The aim of these checklists is to help technical experts understand the technical basics of PETs and the legal considerations involved.

7.5. Improving Education

Solution	Interviewees	Mentions
Law curriculum	(I-2), (I-3), (I-5), (I-7), (I-8), (I-9), (I-11)	7
Training and workshops	(I-1), (I-3), (I-5), (I-6), (I-7), (I-8), (I-11), (I-10)	8
Continuous Learning	(I-1) (I-2), (I-3), (I-4), (I-6), (I-14), (I-15)	7

Table 7.6.: Improving Education

7.5.1. Law Curriculum

It is crucial for legal experts to have a basic technical knowledge of PETs. This is necessary for their legal assessment. Therefore, the training of legal experts on PETs should be improved. One solution strategy that was often discussed in the interviews could be to refine the legal curriculum. Seminars and courses could be introduced into the law curriculum. "*But especially with regard to the studies, it would perhaps make sense to have something like this in the context of a seminar*" (I-7). A dedicated seminar could provide law students with the basics of privacy technologies. Another approach is an interdisciplinary degree program. The gap between law and technology can be bridged more effectively by integrating the two subjects:

> You need a better symbiosis or cooperation between law and technology. The head of the unit has always said that we need a mixed degree, or privacy, or even privacy as a major. (I-7)

Some universities have already begun to combine privacy law with computer [55]. Such interdisciplinary courses could provide a comprehensive understanding of both fields. "*There are already a few, at least at Saarland University, that combine data protection law with IT.*" (I-7) To improve cooperation between technical and legal experts, practical exposure can help to understand technical concepts. One interviewee shared his experience of teaching basic coding to lawyers:

> And I told them at the time that they don't have to be able to reproduce it in depth, but if they are enthusiastic about IT law and have these concepts in their heads, it helps them a lot to evaluate it. I also got the impression that it worked quite well. So it doesn't have to be a brutal deep dive, but just having that basic understanding helps. (I-2)

Legal professionals do not need to become expert programmers, but a basic understanding of technical concepts can improve communication with technical experts:

> Another idea is to include specialized training modules in the curriculum that focus on legal tech. For those particularly interested in the intersection of technology and law, universities could offer elective courses or "additional subjects," as one expert suggested. (I-5)

They do not have to become technical experts. A basic understanding can be very useful. "*But every privacy lawyer should already know a few basic terms.*" (I-1)

The transition from theory to practice is also important. The Royal Society sees the inclusion of internships and work placements in organizations specializing in PETs as a gateway for new graduates [22]. It is a way to seamlessly combine academic knowledge with real-world application, ensuring that fresh insights from academia find their way into the evolving landscape of PET research and development [22].

7.5.2. Trainings and Workshops

Another solution strategy for educating legal professionals about Privacy-Enhancing Technologies is specialized training and workshops. Some law firms offer in-house training. For example, one law firm as it is mentioned by one legal professional took proactive measures. The firm provided IT training programs to the legal experts:

> They have also given us appropriate IT training. So I'm also an ISO 27001 auditor of the deficient type. At that time, we were offered a course and paid for a course, so these are, as I say, already such points that help a lot. Yes, and that is something, you just have a huge advantage over someone who only had the legal training and nothing else. (I-5)

Another interesting insight was the idea of using innovative training formats such as hackathons. These allow legal practitioners to delve deeper into the practical applications of PETs. One legal expert mentioned how they have held hackathons to explore applications such as ChatGPT, turning it into a learning experience:

> For people, we do hackathons where we say let's try this out. We are here at the law firm and we have pizza. Then we spent a day today thinking about what we could do with ChatGPT. (I-3)

Similar approaches could be taken with Privacy-Enhancing Technologies. Such workshops can help to explore the practical applicability of PETs for data privacy compliance.

It is also important to support continuous learning and awareness of PETs. This can be achieved through internal training sessions such as Tech Talks, where emerging technical concepts are discussed. This idea came from a law firm that has implemented a continuous education and awareness strategy:

> We do internal training. And this internal training is for the departments with technical topics, but also for the entire firm. There are monthly Tech Talks, where somebody spends a quarter of an hour at lunchtime explaining what Chat GPT is, what an NFT is, and what that is. So I think we need that technical know-how. We have a department that does that, so they really try to address the legal technical issues that come up. (I-3)

Sessions like these can help educate legal professionals about complex issues and make them accessible to legal professionals without deep technical backgrounds.

But it is not only training on the technical side of Privacy-Enhancing Technologies that can build the capacity of legal experts. It is also mentioned that business training can give legal experts a broader understanding of the use of PETs and the considerations that an organization needs to make. One legal expert explained that this helps to provide advice that is both legally and economically sound. Similarly, training that combines technical, business, and legal contexts can be valuable. Therefore, institutions may also consider introducing specialized training such as the "*technical-economic supplementary training (TWZ)*" (I-5). Such training can provide an understanding of how to balance technical, legal, and economic aspects.

In the end, it's often just a matter of "*learning by doing*" (I-4), which emphasizes the value of hands-on experience. Hands-on workshops that simulate real-life scenarios can be very important. For example, it can be beneficial to have workshops at the beginning of projects where the technical and legal sides educate each other about their requirements.

7.5.3. Continuous Learning

This strategy is based on the findings of several interviews, which revealed that legal experts must have both the mindset and the resources to educate themselves. Being a legal expert often requires a high degree of adaptability. Especially in privacy law, they are often exposed to new technologies and products. These topics were often not part of their formal education:

> You learn to go through an insane amount as a lawyer. I learned outsourcing and technology by outsourcing and negotiating contracts for months. You can't teach that in formal courses. Unfortunately. (I-4)

This underscores the invaluable role of continuing education. Technological advances make it essential for legal professionals to be on the cutting edge:

> And if you don't keep up with the technology, you're going to be left behind. So it's just the case that you can't close yourself off from it because otherwise, you're just going to go under in that area. (I-5)

This quote underscores the need for legal professionals to adapt to technological change and learn to be flexible. Each project or case may require a different kind of technical understanding.

> It may be that tomorrow a new project comes along and I have to completely familiarize myself with it. Then I really work my way in until I understand the product. (I-6)

This iterative process of delving into the technical details of each case ensures that legal advice is accurate and effective. Learning often involves working with technical experts, as one interviewee noted:

> You learn and then you go and talk to the engineers and you become an expert, right? So that is the concept, but instead of for each different case, I continue to delve into those details. And I think part of it is not being afraid to try to understand the details, not being afraid to ask questions and maybe the technical people will say, "Oh, well, that's kind of a stupid question." Whatever it is, I think it's not being afraid of it, not being afraid of it in the first place, right? (I-15)

The quote emphasizes the importance of being open to new technologies and willing to learn.

It is natural for anyone to be afraid of venturing into unfamiliar territory. However, one interview emphasizes the "*importance of curiosity and fearlessness in the learning process. And I think part of that is not being afraid to try to understand the details, not being afraid to ask questions.... I think not being afraid of it at all, right?*" (I-15)

A big problem in all of this is the lack of education, training, and workshops on PETs. "*So there's actually very little in that area. Work material.*" (I-5) Law firms and institutions should invest in creating comprehensive educational materials, both for internal use and for the broader legal community.

7.6. Enhancing Guidance

7.6.1. Legal Applicability

Regulators are very reluctant to provide guidance on Privacy-Enhancing Technologies. This problem relates to the challenge of case-by-case assessment. In the end, every use case is different, and it is very difficult to find a universal strict approach to the use of PETs. In the end, the responsibility would lie with the supervisory authorities. This is why there is very little guidance on controversial new areas such as PETs. Despite the high demand from industry. The importance was mentioned several times in the interviews:

Solution	Interviewees	Mentions
Legal applicability	(I-1), (I-2), (I-3), (I-4), (I-5), (I-6), (I-8), (I-10). (I.11), (I-13), (I-14), (I-15)	12
Improving collaboration	: (I-1), (I-2), (I-3), (I-4), (I-5), (I-7), (I-8), (I-10), (I-11), (I-14), (I-15)	11

Table 7.7.: Enhancing Guidance

> Maybe briefly, why is it very, very important? Because it's a relatively new area of law and a lot of it is still open to interpretation and implementation. And that's often the case with regulators. Of course, they have to be careful, of course, they know how business works, and they don't want to stifle it, but at the same time, they have to follow the law. Often they are not 100% clear, they are a little bit vague, and you have to interpret yourself how far you can go. (I-10)

> I think concretely in Germany it would help if you had clear guidelines on the part of the authorities and on the part of the courts with things to understand, and that again is related to, maybe that's a statement that helps you, that there are more resources in terms of how the authorities can advise on data protection. (I-10)

Clarity from supervisors and regulators on PETs is important to assist organizations, particularly legal professionals, in selecting and evaluating PETs for privacy compliance. Especially for new technologies, it is essential to provide guidance to organizations at the outset to support their use. The lack of use cases, court rulings, and standards increases the need. Regulators and supervisory authorities are seen as the main sources for legal experts to determine the applicability of new technologies, as mentioned earlier:

> Yes, I would say publications from regulators, from the European Data Protection Board, and things like that are the main sources. (I-5)

These sources give legal experts confidence and reliability in selecting PETs. As one interviewee explained, "*because it gives me the authority to invent these manufacturers, and the Federal Office says this is the way it fits, then it gives me the authority to tell my clients, there has to be something better first*" (I-3).

There is a lack of guidance on several aspects of Privacy-Enhancing Technologies. The most challenging are the open legal terms discussed in the legal and regulatory challenges. At the heart of the issue are the definitions of pseudonymization and anonymization. There is an ongoing debate about what is considered personal, anonymous, or pseudonymous. Several

experts have highlighted this challenge. There is a need for "a well-defined metric to assess the level of privacy". There is a lack of clarity and real-world examples:

> And this is a big problem for many. Dealing with anonymized data, how that works, and so on. This is also all that needs to be worked out by the scientific regulators and so on. And even now, after five years, people are still relatively uncertain in many areas. (I-5)

There is also a need for guidance on the risk assessment of PETs. There needs to be clarity on how PETs can help to reduce high-risk processing to a low-risk level:

> They just need to be measures that are taken after 20 or 32, so TOMS classically, need to be appropriate to minimize a risk. Yes. And I have to prove that somehow. If I say in advance that I have a high risk because I have five billion records and two million people are affected. And then I can show or prove afterward that my PET makes sure that the data is less and fewer people are affected, then the risk is also less. So, with that, I would have such a recourse to say that the measure is suitable to minimize the pre-existing risk and therefore it is a valid measure. But that has to be proven. (I-12)

Privacy-Enhancing Technologies are still evolving. In order for legal professionals and organizations to remain compliant, they need to stay abreast of the current state-of-the-art. A list of current state of the art Privacy-Enhancing Technologies can help:

> And then I give it back and then make the mark and say, okay, check. And would such a knowledge, such a list from an authority be interesting? (I-5)

Looking at the literature, the Royal Society highlights the critical role of data protection authorities in promoting PETs and ensuring transparency in algorithms [22]. For these authorities to be effective, they need a technically skilled workforce and a consistent approach in line with European data protection values [22]. In addition, the Royal Society proposes a national strategy focused on PETs that addresses safety needs, promotes international collaboration, and supports scientific research. To be effective, it should be integrated with current national data and AI strategies [22].

7.6.2. Improving Collaboration with Regulators

In order to support legal experts on the use of PETs, cooperation with supervisory authorities needs to be strengthened. Regulators have a mandate to advise on data privacy compliance, but this is often not the case:

> I've never seen, even when I've talked to other colleagues, that the regulators are willing to enter into a discussion because they're not really willing to do so. What is really missing is this discussion and this conversation at eye level. (I-11)

One way is to foster open dialogue through regular forums that bring together legal experts, businesses, and regulators. Such cooperation could build trust among participants. In addition, transparent communication is essential. It is also important for these authorities to proactively engage with industry experts to ensure that they are aware of the specific challenges facing the sector.

To ensure that regulatory policies remain relevant, authorities should establish systems that allow them to receive feedback on their policies. This would ensure that the regulatory landscape evolves with the pace of technological advances in data protection:

> Yes, so it would be nice to have some consolidation and not have it all solved at the state level. So that makes it very difficult. (I-5)

One innovative approach to cooperation between legal experts and authorities is regulatory sandbox systems. These systems provide a "safe environment and testing ground to pilot pet projects" [36]:

> And the only thing I've really seen so far are these sandbox systems, where they're really trying to concretize and already legally pass on what the system has to look like. (I-7)

> Anonymization is no longer the most important issue because you have a closed network. If you implement that hard, if you really don't have a network connection to your home, then a lot of protection is no longer necessary. (I-7)

In this way, legal experts can observe how these technologies work and where privacy compliance challenges arise. They also gain hands-on experience with PETs. This is very valuable in understanding how PETs interact with existing legal frameworks. Regulatory sandboxes often involve collaboration between innovators, regulators, and legal experts. Insights from sandbox testing can inform and shape future regulations and standards. Legal experts can then make informed recommendations to regulators. By better understanding the practical applicability of PETs, legal experts can better advocate and communicate the benefits and risks of these technologies [22].

8. Mapping PETs and Data Protection Principles

8.1. Procedure

During this research, it became clear that the legal applicability of Privacy-Enhancing Technologies ist still unclear regarding several aspects. Legal experts need to align PETs to the legal requirements regarding technical measures. As often discussed, new technologies need to be assessed according to the data protection principles in Article 5. An important reference, from which the idea for this artifact originated, is the ICO PETs Guidance [9]. This report maps Privacy-Enhancing Technologies to the data protection principles. In another source for this thesis, the Standard Data Protection Model, protection goals based on the data protection principles of the GDPR are mapped to the legal requirements of the technical design of processing activities. The first artifact maps these legal requirements from the Standard Data Protection Model [33] to the data protection principles from the GDPR [7]. These principles are then, according to the mapping from the ICO report [9], aligned to the Privacy-Enhancing Technology that helps to fulfill this data protection principle. This mapping is grounded from the two mentioned sources and the best assessment of the author. The findings of this mapping were validated in an interview with a regulator. In prior interviews the usability and need for a mapping from the data protection principles to Privacy-Enhancing Technologies became clear:

> The Data Protection Model is something we can hang our hats on. It has very general measures. There are these privacy objectives, as you have read, such as confidentiality. And if a PET or a technical mechanism is suitable to achieve these protection goals, i.e. to modify a technology to improve its ability to achieve the protection goals, then it is also intended for compliance, so to speak. And then it can be used for that purpose. I just have to be able to somehow prove that the technical mechanism that I have will help to achieve a legal objective. And that proof is necessary. (I-12)

> What's important for touch sharing is actually where this technology helps to achieve a certain data protection principle or style of protection. So just this mapping to data minimization or pseudonymization or access restriction, that mapping always has to be there in order to be able to say if is it useful or not. And I think you can do that for legal texts on a relatively abstract level. If you

> make it clear that it has been proven and that it works, you don't have to go into technical depth, but you can describe it conceptually and make clear why it works and make clear why this is helpful for a particular data protection principle or privacy goal. (I-12)

In the second part, it is described how each Privacy-Enhancing Technology can achieve the corresponding data protection principle. The data protection principles are categorized according to their legal requirements which are detailed described in the Standard Data Protection Model [33]. The legal requirements of each data protection principle are then mapped to the according PET and its technical functionality. The explanations of how the according PET can achieve its data protection principle are based on literature and an email correspondence with the Information Commissioner's Office. The mapping of the legal requirements to the functionality is made by the best assessment of the author.

To validate the artifact, an interview with a regulator was conducted. This helped to improve the mapping and clarify further uncertainties in the explanations. Also, two legal experts were consulted to gain more insights on the usability of such a mapping:

> No, it is great. Yeah, I can, I can totally understand that. I think that is cool, too. I think it also has a real scientific value, because in risk analysis, for example, it can sometimes come out that, okay, the data processing in question is basically fine, but we are processing far too much data. For example, the child's birthday, that maybe we do not need a personnel action. Now one could ask the question, hey, which mitigating measure, which PET could I use? And then you can say, okay, Secure multi-party computation, whatever that means. But if you say you have the tool, I think that is a really cool idea. (I-8)

> Also, if I say, I have data minimization somewhere, I just want to use the data and as little as possible, as much as I need and as little as possible, then I look at what technologies I can use to do that. [I-5]

8.2. Artifact

Data Protection Principles and their Legal Requirements

A: Purpose Limitation

1. Data must only be processed for the purpose it was initially collected for
2. Any further processing must align with the original purpose and consider the processing context
3. If processing extends beyond the original purpose, affected individuals should be informed and can exercise their right to object

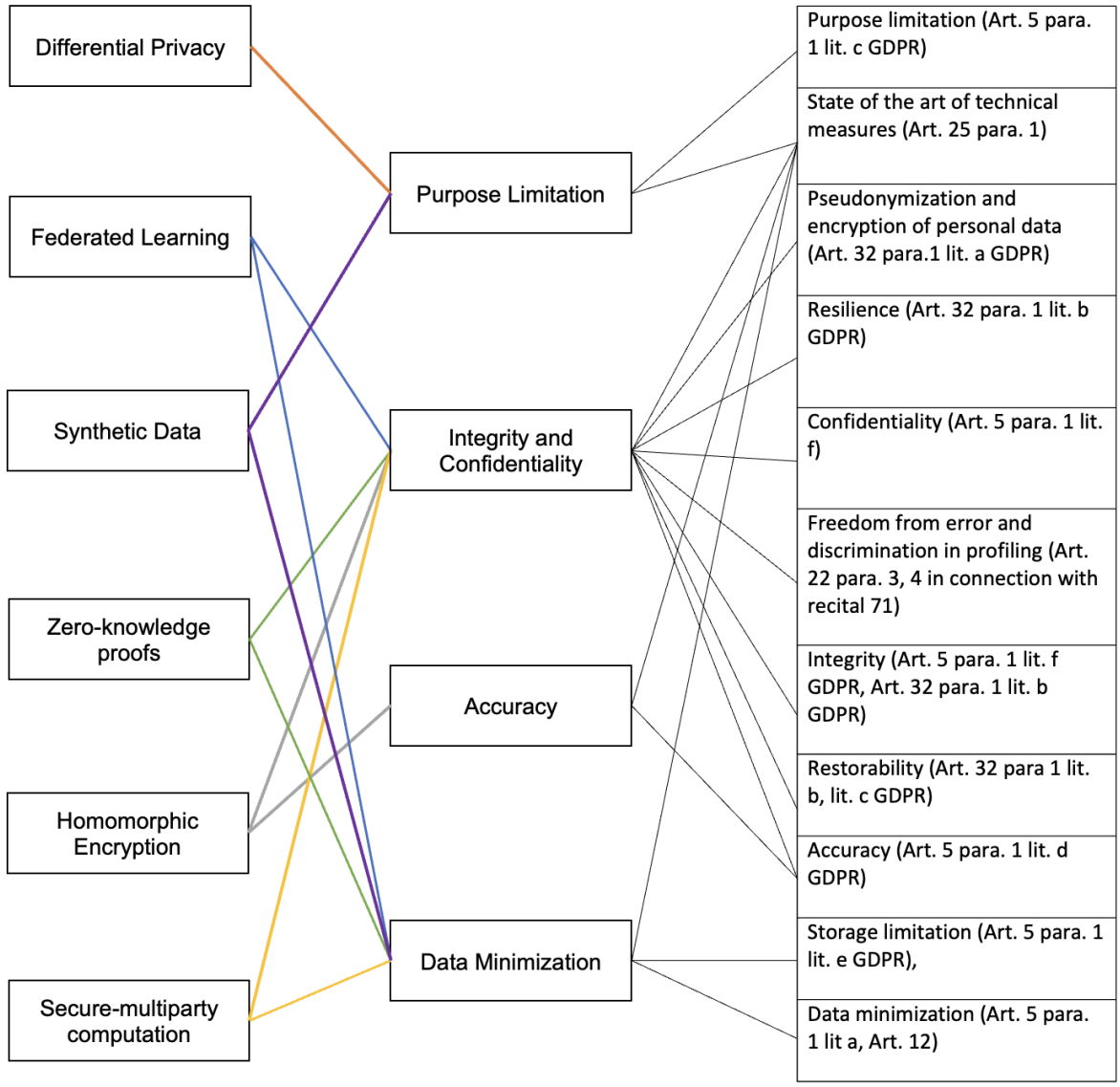

Figure 8.1.: Mapping Data Protection Principles and PETs

B: Data Minimization

1. Data Minimization mandates that personal data must be adequate, relevant, and limited to what's necessary for processing
2. Little to no personal data should be processed, and it should be considered before and during processing
3. Technical and organizational measures should ensure processing stays within pre-set boundaries

C: Accuracy

1. Data used in processing should be accurate and updated as needed
2. All reasonable measures should be taken to promptly erase or correct any inaccurate data relative to its processing purpose

D: Confidentiality and Integrity

1. Appropriate security measures are required to protect personal data
   1.1. Integrity
      1.1.1. Protection against unauthorized modifications and deletions of personal data
      1.1.2. Personal data processing must ensure protection against accidental loss, destruction, or damage using appropriate technical and organizational measures
      1.1.3. Unauthorized changes to stored data should be prevented or at least detectable for rectification
   1.2. Confidentiality
      1.2.1. Unauthorized individuals should not access or use data or the devices processing it

Privacy-Enhancing Technologies and Data Protection Principles

Homomorphic Encryption	
Confidentiality and Integrity	Homomorphic Encryption helps to ensure the data protection principle of Confidentiality and Integrity (Security) [9]. Homomorphic Encryption enables computations on encrypted data. The data remains in an encrypted state at rest, in transit, and in the entire computation process [56]. Hence, Homomorphic Encryption protects against unauthorized access and usage of the data because the users would only have access to the encrypted data, which is useless without the decryption key [57]. (D1.1.1, D1.1.2, D1.2.1) In the case of an alteration of the encrypted data, it would result in a failure to correctly decrypt. This makes unauthorized changes at storage or computation detectable for rectification [56]. (D1.1.3) In general, Homomorphic Encryption pseudonymizes data and can therefore be seen as an appropriate security measure to protect personal data [57]. (D1)
Accuracy	Homomorphic encryption help to ensure the data protection principle of accuracy [9]. This is achieved by the ability to perform computations on encrypted data without needing to decrypt it. The result, once decrypted, is as accurate as if the computation were performed on the original unencrypted data. (C1) This ensures an accurate result [21]. By maintaining data in an encrypted state during storage and computations, homomorphic encryption can help preserve data integrity by preventing unauthorized alterations to the data. Even if the encrypted data were to be tampered with during computation or transmission, it would not decrypt correctly, so that all inaccuracies can be corrected [57]. (C2)

Table 8.1.: Homomorphic Encryption

Differential Privacy	
Purpose Limitation	Differential Privacy help to ensure the data protection principle of purpose limitation by achieving anonymous data. It has to be considered whether or not there is a risk of reidentification. This is achieved by adding a randomized injection of noise to the data. When implemented correctly, the risk of re-identification can be significantly minimized, making anonymization a realistic outcome. Nevertheless, it is crucial to note that companies must possess a legitimate legal basis for conducting the anonymization process [27]. The principle of purpose limitation asserts that personal data should only be processed for the purpose it was collected. By anonymizing personal data to a degree where the risk of re-identification is negligible, we highly limit any direct links to previously personal information and therefore minimize the risk that personal information can be used for further purposes. Differential Privacy can achieve this by using an appropriate privacy budget, which controls how much noise is added to the data. This noise is random data that is added to the true response of a query. It protects individual data points from being re-identified (ICO, e-mail exchange). (A1, A2, A3) It is important that companies can prove that individuals are no longer identifiable. They must ensure that the anonymized data is robust against the risks of singling out, linkability, and inference [58]. In conclusion, you can remove the identifiability of individuals with the help of Differential Privacy. There is no longer a link in the data to the original personal information. This means the data is no longer tied to the purpose for which it was collected, freeing it for secondary usage.

Table 8.2.: Differential Privacy

Synthetic Data	
Data Minimization	Synthetic data help to ensure the data protection principle of Data Minimization [9]. Synthetic data is 'artificial' data that is generated from real data. You can use Synthetic data to generate large datasets from small datasets. It reproduces its patterns and statistical properties. Hence, generating synthetic data guarantees adequate, relevant, and limited data usage [57]. (B.1) Synthetic data can achieve that little to no personal data is processed, and therefore Data Minimization is achieved [57]. (B2)
Purpose Limitation	Synthetic data helps to ensure the data protection principle of purpose limitation by achieving information that is anonymous (ICO e-mail exchange). It is important to consider whether or not there is a risk of reidentification [58]. The principle of purpose limitation mandates that personal data should only be processed for the purpose for which they were collected. Synthetic Data provides a way around this limitation by creating 'artificial' data that does not directly relate to any specific individuals. This unlinked data can be used for further purposes because the personal information cannot be re-identified (ICO, e-mail exchange). (A1, A2, A3)

Table 8.3.: Synthetic Data

Secure-Multiparty Computation	
Data Minimization	Secure-multiparty computation help to ensure the data protection principle of Data Minimization [9]. Secure-multiparty computation is a protocol that allows at least two different parties to jointly process their combined information. The result is computed by combining their data without disclosing the nature or content of their private inputs [57]. Secure-multiparty computation ensures that the amount of data you share is limited to what is necessary for your purpose. Only the output is revealed. Hence, the data usage is adequate, relevant, and limited to what is necessary for processing [59]. (B1, B2)
Confidentiality and Integrity (Security)	Secure-multiparty computation help to ensure the data protection principle of Confidentiality and Integrity (Security) [9]. In Secure-multiparty computation, each party contributes a private input to compute a function. Due to this collaborative process, the result can only be determined from the collective inputs of all parties. Also, the parties share only a function where no personal information can easily be derived from [59]. Hence, the risk of unauthorized individuals gaining access to or using personal data is significantly decreased. (D3.1) Also, any significant change to the computation process and therefore output would require having influence on most of the inputs, which is highly unlikely. Therefore, the protection against, changes, destruction, or deletions of personal data is very high, and the potential damage of a data breach is significantly limited [59]. (D2.1, D2.2, D2.3)

Table 8.4.: Secure-Multiparty Computation

Zero-knowledge proofs	
Data Minimization	Zero-knowledge proofs can help to ensure the data protection principle of Data Minimization. ZKPs is a protocol where a prover can prove to a verifier that they know a specific piece of information, without sharing the information itself or any additional details with the other parties. This inherently supports Data Minimization because only data that is adequate, relevant, and limited to what is necessary to give a proof is used [9]. (B1) Hence, little to no personal data is processed. (B2) Because ZKPs allow a prover to demonstrate knowledge of information without revealing it, they can reduce the need for storing sensitive information. Once a fact is proven using a ZKP, there is not the need to keep the underlying data which helps with the earliest possible erasure of data [57]. (B3)
Confidentiality and Integrity - Security	Zero-knowledge proofs can help to ensure the data protection principle of Confidentiality and Integrity (Security). By allowing a prover to prove to a verifier that they know a value without revealing sensitive information itself, personal data remains secure and confidential. Because ZKPs require no exchange of the actual sensitive data during the proof, the attack surface for potential data breaches is minimized [57]. Unauthorized individuals would only have access to the proof without the underlying sensitive information. (D1.2.1) Consequently, there is also no possibility of altering, damaging, or deleting personal information. (D1.1.1, D1.1.2, D1.1.3)

Table 8.5.: Zero-knowledge proofs

Federated Learning	
Data Minimization	Federated Learning helps to ensure the data protection principle of data minimization [21]. Federated Learning allows multiple different parties to train AI models remotely with their own information. These so-called local models combine some of the patterns that they have identified (known as 'gradients') into a single, more accurate global model, without having to share any training data with each other. This collaborative training is repeated until the centralized model is fully trained [60]. Therefore, the local model only has access to its own data which minimizes the processing of personal information by the centralized model. (B2) The raw data stays at the different parties [9]. (B1)
Confidentiality and Integrity - Security (in combination with other PETs)	Federated Learning help to ensure the data protection principle of Confidentiality and Integrity (security) [9]. Federated Learning distributes the computation process to multiple different parties. Hence, the data remains localized on the device or server it originates from and does not need to be transferred to a central server for processing. This reduces the risk of data breaches during storage and data transfer. Also, it decreases the impact if the central server is compromised. Hence, the protection of data from unauthorized access, use, alteration, or deletion is significantly enhanced [60]. (D1.11, D1.1.2, D1.1.3, D1.2.1) As described, the risk of re-identification can be reduced by training the centralized model, but the local models can still contain personal information. Hence, Federated Learning should be combined with other PETs to guarantee a low risk of re-identification at every stage in the AI training process (ICO, e-mail exchange). To support the security principle, Federated Learning can be combined with other PETs: SMPC protects parameters that are sent from the clients to ensure that they do not reveal their inputs (ICO, e-mail exchange). Homomorphic Encryption can encrypt local model parameters from all participants (ICO, e-mail exchange). Differential Privacy can hide the participation of a user in a training task (ICO, e-mail exchange).

Table 8.6.: Federated Learning

9. Challenges - Solutions Mapping

This figure maps the identified challenges to the presented solution strategies. This mapping is based on the qualitative analysis. The figure serves only as an overview of the applicability of the identified solutions to the corresponding challenges. More research needs to be done on the practical implementation of the proposed solution strategies. This will be necessary to better understand the interrelationship between the challenges and the corresponding solutions.

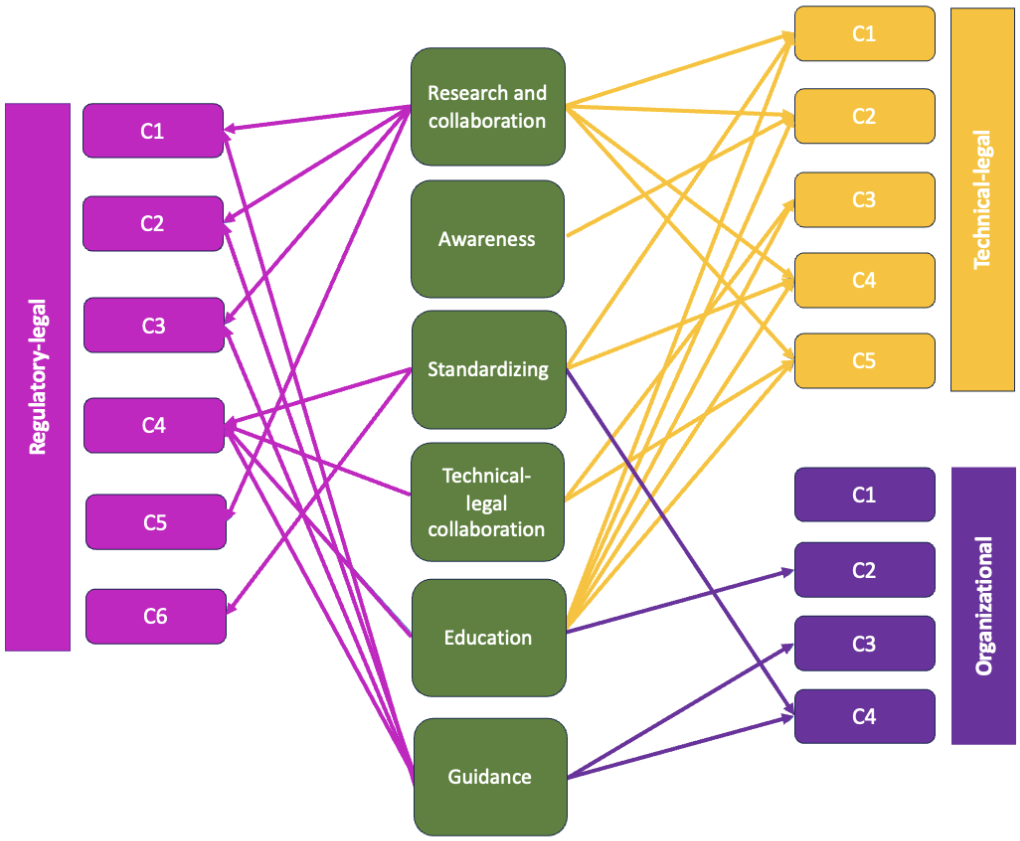

Figure 9.1.: Challenges-Solutions Mapping

10. Discussion

10.1. Limitations

In my research efforts, I encountered certain limitations that must be considered in the context of my work. The limited number of legal experts interviewed results in an unrepresentative view and may result in certain areas and issues remaining undetected. Therefore, the results are not generalizable and the dependence on the answers and feelings of the respondents may affect the objectivity of the study. In addition, I only collected the data over a three-month period, so other developments may have occurred in the meantime that were not considered and could affect the depth and breadth of the study. Future researchers are advised to validate the findings through further qualitative as well as quantitative research that includes a larger and more diverse data set to increase the validity and relevance of the findings. In addition, the majority of respondents were located in Germany. To get a more holistic view of data privacy compliance, legal experts from different countries should be interviewed.

10.2. Future Work

Legal Applicability of PETs:

- Anonymization vs. Pseudonymization: Exploring which PET can function as pseudonymization or anonymization technique.
- Risk Metrics: Develop standardized criteria to evaluate Privacy-Enhancing Technologies as risk mitigation measures.
- Use cases: Exploring the use cases for Privacy-Enhancing Technologies in different industries.

Education and Training:

- Education Modules: Design of education programs to inform legal professionals on Privacy-Enhancing Technologies.
- Interdisciplinary studies: Exploring mixed studies of law and technology.

Technical-Legal Cooperation:

- Interdisciplinary Training: Explore programs and methodologies for cross-training technical and legal experts.
- Tool Development: Creating tools that are designed to guide legal experts through technical aspects of PETs and tech professionals through legal implications.
- Technical-Legal Frameworks: Exploring organizational frameworks for the collaboration of technical and legal experts.

Organizational Factors:

- Organizational Culture and Privacy: Explore how an organization's data privacy culture can be fostered and manifested.
- Integration with Business Strategy: Investigating how data privacy compliance can be integrated into the broader business strategy.

11. Conclusion

The role of legal experts has grown in importance in recent years with the emergence of modern data protection regulations such as the GDPR. One of the requirements of these regulations is the use of technological measures to protect the personal data of data subjects. Privacy-Enhancing Technologies can serve as these technical measures. To ensure compliance, they must be evaluated by legal experts for their applicability in light of the latest legal requirements. Legal experts evaluate Privacy-Enhancing Technologies according to data protection principles and various aspects related to the technical measures, such as the state-of-the-art or the risk of processing.

In this work, several challenges that legal experts face in the process of data privacy compliance with PETs were identified. They were classified into three groups: legal-regulatory, technical-legal, and organizational. It became clear that one of the biggest challenge is the unclear legal and regulatory landscape. The lack of case law, standards, and guidelines for Privacy-Enhancing Technologies exacerbates this challenge. In addition, it was found that awareness and knowledge of Privacy-Enhancing technologies in the legal field remain low to this day. This knowledge gap is one of the biggest challenges in the collaboration between legal experts and technical experts. While legal professionals do not need to be technical experts, they do need a basic technical understanding and the ability to evaluate the use of Privacy-Enhancing Technologies. When assessing the legal applicability of Privacy-Enhancing Technologies, they often need to rely on the expertise of technical departments.

To overcome these challenges and obstacles, several solution strategies were identified and explored. Guidance from regulators is needed to help legal professionals navigate in the unclear legal landscape for Privacy-Enhancing Technologies. In this context, standards and certification can also help to bridge the gap between legal requirements and the adoption of Privacy-Enhancing Technologies. Collaboration between legal experts and technologists also needs to be encouraged. Organizational structures can help create cross-functional teams and predefined processes to support collaboration between these departments. As they collaborate, they need to find a common language to bridge the gap between their different domains. Therefore, technology training should be improved to enhance legal professionals' technical knowledge and expertise on PETs.

The applicability of data protection principles to selected PETs has been investigated. Their usability to these principles was confirmed and explained. Further research is needed to examine the applicability of PETs to other legal requirements in order to increase their usage for data protection compliance.

According to the interviews, the use of Privacy-Enhancing Technologies will inevitably increase over time. There will be case law, case studies, and further guidance. Privacy-Enhancing Technologies offers a unique opportunity, particularly in sensitive areas such as healthcare, to protect privacy while at the same time enabling data-driven business cases. However, both businesses and regulators should be more open to technical innovations for data privacy compliance. Bringing law and technology together is considered the most critical and overarching challenge and will set the stage for Privacy-Enhancing Technologies to reach their full potential.

Overall, legal experts have an important role to play in bridging the gap between technology and law. These areas need to be brought together at multiple levels to facilitate the use of Privacy-Enhancing Technologies in complying with data protection regulations.

A. General Addenda

A.1. Questionnaire

The interview questionnaire is included below.

A.2. Quotes Translations

Interviewe	German quote	English translation
I-3	So, jetzt hat sich es aber durch DS-GVO und andere Regelungen sehr stark ins Juristische gezogen, so dass ITler da manchmal an ihre Grenzen stoßen, wo es einfach um die juristische Bewertung geht.	But now, due to the GDPR and other regulations, it has become a legal matter very much, so that the IT staff sometimes reach their limits when it comes to the legal evaluation.
I-6	Aber das ist immer unternehmensabhängig, sag ich mal, wer tatsächlich auftaucht. Ja, das ist das Ding, das variiert natürlich extrem. Alles variiert extrem.	It always depends on the company; I would say it depends on who shows up. Yeah, that's the thing, it varies extremely, of course. Everything varies extremely.
I-15	Wir arbeiten viel mit Legal Departement zusammen, weil das auch so ist, dass wir bei der Vertragsgestaltung, Also die haben auch Basiswissen, oder auch erweitertes Wissen, aber kein Spezialwissen im Bereich Datenschutz. Das heißt, wir sind da stark vernetzt.	We work relatively much with the legal department, because that's also how we draft contracts, they also have basic or advanced knowledge, but no specialized knowledge in the area of data protection. That means we are relatively strongly networked

I-3	Wenn ich das also weglasse, habe ich ein etwas höheres Risiko, aber wie hoch ist das Risiko? Das ist letztlich die Entscheidung, die aus meiner Sicht die verantwortliche Person treffen muss. Und als Datenschutzbeauftragte können wir nicht sagen, das ist nicht möglich, sondern es gilt die so genannte Business Judgement Rule. Das heißt, das Unternehmen muss entscheiden, wie viel Risiko akzeptabel ist.	“So if I leave that out, I have a little bit higher risk, but what is the risk? That’s ultimately the decision that, from my point of view, the responsible person has to make. And as data protection officers, we can’t say that’s not possible; instead, the so-called business judgment rule applies. That is, the company must decide how much risk is acceptable
I-8	ist eine Art Richtungsgeber, der letztlich auch für den Datenschutz verantwortlich ist.	is a kind of direction-giver who, in the final analysis, is also responsible for data protection." (I-17)"
I-8	Meistens gibt es eine Abteilung, von der das Problem ausgeht.	Most of the time you have a department where the problem comes from.
I-8	Die Abteilung muss sich dann an die IT-Abteilung wenden, die dann sagt, dass sie sich mit diesen Fragen an den Datenschutz wenden muss, und dann ist die Abteilung letztendlich verantwortlich. und in diesem Bereich führend.	the department then has to go to the IT department and they then say you need to go to data protection for these issues and then the department is ultimately responsible. and leading in that area.
I-5	Und natürlich ist es der Gesetzgeber, der letztlich die Rahmenbedingungen setzt.	And, of course, it is the legislator who ultimately sets the framework conditions.
I-5	Vielmehr sind es die Regulierungsbehörden, denn sie haben natürlich die Deutungshoheit über das Gesetz.	The regulatory authorities rather, because, of course, they have the interpretation of the law.
I-5	Datenschutz und IT, also sind so die zwei Hauptrollen, die eigentlich immer eine Rolle spielen. Also dass das andere dazu kommen, das ist dann immer so eine organisatorische Sache, also wie es aufgeteilt ist.	Simply what one exchanges their times. And most of the time, that’s data protection and IT, so those are the two main roles that actually always play a role. So that the others come to it, that is then always such an organizational thing so how it is divided.

I-8	Habe ich tatsächlich mit der Informationssicherheit, oftmals, einen direkten Austausch, dass ich sage, okay, wir haben eine neue Software beispielsweise, die eingesetzt werden soll, die technische organisatorischen Maßnahmen. Habt ihr die schon geprüft? Sollen wir die prüfen? Prüfen wir die gemeinsam? Stimmen wir uns dazu ab?	I have a lot to do with them, then I actually have a direct exchange with their information security, often, a direct exchange, that I say, okay, we have new software, for example, that is to be used, the technical organizational measures. Have you already checked them? Should we check them? Do we check them together? Do we coordinate our efforts?
I-8	Wenn es komplexe technische Sachverhalte sind, komplexe Systeme, dann von Anfang an eigentlich sehr eng. Also dann lasse ich mir das erklären, auch von der Seite, wie funktioniert das tatsächlich in einfacher Sprache, denn es ist auch die Juristinnen und Juristen verstehen. Also da kann es tatsächlich vorkommen, dass wir von Anfang an sagen, okay, das macht uns zusammen. ich würde mal sagen, je komplexer und je technischer der Verarbeitungsvorgang ausgestaltet ist, dass du schneller so auf den Schulter Schluss mit den ITlern an.	If they are complex technical issues, complex systems, then we are actually very close from the start. So, then I have it explained to me, also from the side of how it actually works in simple language, so also lawyers can understand. I would say that the more complex and the more technical the processing procedure is, the quicker the cooperation with the IT people will be.
I-16	Also, das ist, wenn dann oft so, man hat irgendwo was gelesen, was das Tolles Neues geben soll und fragt wir bei IT nach, wäre das nicht auch was für uns?Ja. Also, ich sage mal, bei uns jetzt im großen Unternehmen nicht, weil die sind da so weit voraus. Den kann ich nichts Neues erzählen.	Well, it's often like this: you've read something somewhere that's supposed to be great and you ask the IT, wouldn't that also be something for us? Yes, well, I'd say not in our big company, because they're so far ahead. I can't tell them anything new.

I-8	Das ist okay, ich hab keine Ahnung, was das heißt. Dann rufe ich mal ein ISO an und sag so, hey du, ich hab jetzt die Ansage bekommen, der hat einen Verschlüsselungsmaßnahmen, ist das State of the Art? Und dann sagt er, ja, das ist State of the Art, passt. Und dann gebe ich wieder zurück und macht dann die Markierung	That's okay, I have no idea what that means. Then I call an ISO and say, hey you, I got the announcement now,he has an encryption measure, is that state of the art? And then he says, yes, that's state of the art, it fits. And then I give it back and then he makes the mark...
I-3	Und ja, da wird es auch irgendwann, das ist der letzte Frage der Bewertung und das ist eine Frage, wo der juristische Sachverstand einkommt, wo der Technik-Sachverstand einkommt. Und ganz zum Schluss ist das dann wieder die Business-Judgment rule Es entscheidet der es einsetzt.	And yes, at some point, hat is the last question of evaluation and that is a question of where the legal expertise comes in, where the technical expertise comes in. And at the very end, it's the business judgment rule again. The decision is made by the one who uses it.
I-5	wenn ich irgendwas Neues einführe dass wir haben schon irgendeine Tool, das funktioniert gut und die bringen was Neues raus, dass man das dann auch einsetzen möchte, dass man dann nochmal den ganzen Prozess durchführen muss.	Yes, that's also the point, that when I introduce something new, that we already have some tool that works well and they bring out something new, that they then also want to use, that you then have to go through the whole process again.
I-5	Weil davon hängt natürlich alles ab, also dass man das versteht und das ist auch immer mit der schwerste oder komplizierteste Teil, weil du genau alles umreißen musst, alle Informationen geholt musst, dass du nicht für jede kleine, also jede Prüfung nochmal bei jedem kleinen Problem um Fachbereich laufen musst.	We want to understand exactly what is supposed to be done, because of course everything depends on that, that you understand it and that is always one of the hardest or most complicated parts.
I-8	Und dann ist mir eigentlich fast egal, wie das System heißt und wie das genau im Hintergrund funktioniert, solange ich eben verstehe, wie die Datenverarbeitung funktioniert.	I don't really care what the system is called and how exactly it works in the background, as long as I understand how the data processing works.

I-8	Das damit steht und fällt das Ganze von der Bewertung her. Wenn der Sachverhalten nicht wirklich ausgeforscht ist, dann wird es super schwierig, das zu bewerten.	The whole evaluation stands and falls with the analysis of the facts. If the facts are not really explored, then it will be super difficult to evaluate. In other words, to assess it solidly.
I-1	Da können wir schlecht beraten, weil wir die Technologie nicht kennen. Das ist dieses Thema. Ich kann nicht von Anfang an sagen, ihr müsst so und so machen. Wir brauchen erst so ein bisschen Futter. Wir müssen erst wissen, wie soll dieses Produkt aussehen, und dann können wir es uns angucken.	We cannot give good advice because we don't know the technology. That is the issue. I can't say from the beginning that you have to do this and that. We need a bit of fodder first. We first have to know what this product should look like, and then we can look at it
I-8	ich würde mal sagen, je komplexer und je technischer der Verarbeitungsvorgang ausgestaltet ist, dass du schneller so auf den Schulter Schluss mit den ITlern an.	If they are complex technical issues, complex systems, then we are actually very close from the start. So, then I have it explained to me, also from the side of how it actually works in simple language, so also lawyers can understand. I would say that the more complex and the more technical the processing procedure is, the quicker the cooperation with the IT people will be.
I-5	wir sagen jetzt haben wir den Sachverhalt erfasst jetzt haben wir gesagt okay wir haben grundsätzlich eine Rechtsgrundlage es ist kein Showstopper dabei wo wir sagen esgeht auf gar keinen Fall aber wir müssen natürlich dann trotzdem jetzt noch das Risiko irgendwie erkennen und bewerten	We say we have now grasped the facts, we have a legal basis, there is no showstopper where we say it is not possible at all, but of course we still have to recognize and assess the risk somehow.

I-5	im DPIA schaust du dir dann wirklich Schritt für Schritt an dass du sagst wie agiert der Dienstleister. Er soll mal seine Infrastruktur auflegen deswegen bindest du auch den ITler mit ein, weil der dann genau seine Infrastruktur alles offenlegt und dann ihm beschreibt, was er genau macht. Und dann kannst du auch die Punkte, wo eigentlich das hohe Risiko, weil meistens ist ja das nicht der ganze Prozess	In the DPIA you really have to look at it step by step, that you say how does the service provider act. He should put up his infrastructure, because of that you also involve the IT person, because he will then exactly show his infrastructure and then describes to him exactly what he does. And then you can also find the points where actually the high risk is, because most of the time that's not the whole process.
I-5	dass da dann eben diese Privacy-Enhancing Technologies ins Spiel kommen, dass man da dann sagt, ja, das Risiko ist hoch oder vorhanden. Und durch diese Technologien schaffe ich das Risiko, dass ich eben kein hohes Risiko mehr habe.	This is where these Privacy-Enhancing Technologies come into play, that one then says, yes, the risk is high or present. And with these technologies, I no longer have a high risk.
I-3	Also ich nenne das für Verschlüsselungslänge. Wir haben Zeit, da war 128 hat gereicht. Heute ist oder der Punkt ist heute das BSI sagt heute immer noch 128 reich, aber die Empfehlung ist 256. Mit dem Ergebnis dass die Aufsichtsbehörden sagen, 128 reicht nicht mehr.	So I call that for encryption length. We have time, there was 128 was enough. Today, or the point is today, the BSI still says 128 is enough, but the recommendation is 256. With the result that the supervisory authorities say that 128 is no longer sufficient.
I-8	werden. Also ihr müsst mir als Fachbereich oder auch aus Techies so viel Futter in die Hand geben,dass ihr sagen könnt, okay, ich kann das rechtlich verargumentieren, dann kann das eine Aufsichtsbehörde	So you have to give me as a faculty or also the techies so much fodder in my hand that I can say, okay, I can argue that legally in front of a supervisory authority.
I-5	Was ist das überhaupt? Und ist das gut? Und ist das der Stand der Technik? Der IT-Typ sagt mir dann, im Moment ist es so. Passt. Haken.	What is this anyway? And is that good? And is that state of the art? The IT guy tells me then, at the moment it's like this. Fits. There's a catch.

I-5	Grad eben was sinnvoll ist, dort eben die Maßnahmen einführen, dass eben nicht die die Privacy-Enhancing-Tenology ist irgendwo zu einem Risiko werden, weil ich sie blind Einsätze.	So, the bottom line is, I would also say that it is necessary to introduce measures to the extent that it makes sense. So that the privacy-enhancing technology does not become a become a risk somewhere because I use them blindly.
I-5	Es kann schon sein, aber grundsätzlich, weil da auch auf die Kapazitäten fehlen, ist es so, man gibt die Richtung vor, sagt, was eingesetzt werden soll und umgesetzt werden soll, was zu beachten ist.	"It can be, but basically, because there is also a lack of capacity, it is like this: you give the direction, say what is to be used and implemented, what is to be done and what is to be done.
I-8	Und dann kann es dann schon sein, dass man auch tatsächlich nochmal sich zusammensetzt und das nochmal neu kalibriert und ausgestaltet und dann aber auch tatsächlich Risikoentscheidungen rifft, die aber dann weder Privacy treffen kann, noch IT, noch Marketing, sondern das wird dann eskalieren in Richtung Geschäftsführung, dass man sagt, okay, wir müssen da jetzt eine Entscheidung treffen.	It may be that you actually sit down together again and recalibrate it and shape it and then actually make risk decisions. But then neither privacy, nor IT, nor marketing can meet, but the will then escalate in the direction of the management, so that they will say, okay, we now have to make a decision.
I-8	Ja, also im Kontext der Kalibrierung, klar, dann kann es dann schon nochmal sein, dass man, also die Datenschütze*innen vielleicht sagen, okay, wir gehen ganz, ganz stark nach rechts im Kontext Privacy und dann kommt aber die Marketingabteilung und sagt, nee, auf keinen Fall, ich mach nicht mehr mein Revenue, wir müssen nach links gehen.	Yes, in the context of calibration, of course, it can happen that the data protection officers say, okay, we are going very, very strongly to the right in the context of privacy. in the context of privacy and then the marketing department comes and says, no, absolutely not.

I-3	Und ja, da wird es auch irgendwann, das ist der letzte Frage der Bewertung und das ist eine Frage, wo der juristische Sachverstand reinkommt, wo der Technik-Sachverstand einkommt. Und ganz zum Schluss ist das dann wieder die Business-Judgment rule, es entscheidet der der es einsetzt. Und das können weder die Informatiker noch wir Juristen demjenigen abnehmen, die Eigenverantwortung dessen, was er tut. Also können Definitionsbegriff geben. Aber im Ergebnis werden wir immer sagen müssen, vielleicht gibt es noch einen, der das anders sieht und der das weiter anders sieht, dass Risiko musst du jetzt in Kauf nehmen.	And yes, at some point, hat is the last question of evaluation and that is a question of where the legal expertise comes in, where the technical expertise comes in. And at the very end, it's the business judgment rule again. The decision is made by the one who uses it. Neither the computer scientists nor we lawyers can take that away from them, the personal responsibility of what they do. We can give him definitions, terms of definition. In the end, we will always have to say that maybe there is someone else who sees it differently, and you have to accept that risk.
I-7	Aber es kommt immer noch relativ häufig vor, zumindest ist das meine Wahrnehmung, dass Unternehmen auf uns zukommen, noch bevor sie etwas tun. Es gibt sicherlich auch viele Unternehmen, die das nicht tun. Aber wir bestellen eigentlich relativ oft, wenn es Unsicherheiten gibt, kommen sie zu uns und fragen uns, okay, reicht das?	But it still happens relatively often, at least that's my perception, that companies approach us even before they do something. There are certainly also many companies that don't do that. But we actually order relatively often when there are uncertainties, they come to us and ask us, okay, is this enough?
I-4	Aber das ist auch, dass ich mindestens 90 Prozent der Arbeit, die im Rahmen von Dokumentation schließe.	But that's also to say that I do at least 90 per cent of the work that is done in the context of documentation.

I-4	der zweite Teil, wo der Jurist ins Spiel kommt, das sind die Dokumentationsthemen. Wenn du denkst, dass die ganze Dokumentation im Endeffekt, ja, muss man sagen, für die Aufsichtsbehörde Gemacht wird zur Verteidigung, vor Aufsichtsbehörden ist eswichtig, dass Juristen drauf schauen, um zu verstehen, ist das die Sprache, die eine Aufsichtsbehörde versteht.	The second part where the lawyer comes into play, that's the documentation issues. If you think that all the documentation in the end, yes, one must say, for the supervisory authority. It is important that lawyers look at it to understand whether it is the language that a supervisory authority understands.
I-8	Und jetzt sind wir natürlich auch mit den Aufsichtsbehörden konfrontiert. Die schicken uns einen knallharten Fall und sagen, wir gehen von diesem und jenem aus und jetzt, liebe Firma, beweist ihr mir jetzt das Gegenteil. Und das sind wirklich, teilweise haben Sie das gemerkt, das ändert sich jetzt ein bisschen, also 2018, 2019 waren die Fragen noch sehr grundsätzlich. Also haben sie ein Datenschutzmanagementsystem? Ja. Und jetzt fragen sie eigentlich schon, okay, wie setzen sie die Rechenschaftspflicht im Rahmen des Prozesses um? Sie gehen also jetzt sehr ins Detail.	And now, of course, we are also confronted by the supervisory authorities. They send us a hard and fast case and say that we assume this and that and now, dear company, you prove me now wrong. And those are really, partly you noticed that, that's changing a bit now, so 2018, 2019 the questions were still very basic. So they have a data protection management system? Yes. And now they are actually already asking, okay, how do they implement accountability in the context of the process? So they're going into a lot of detail now.
I-8	Dann könnte ich im schlimmsten Fall vor Gericht gehen und sagen, Das ist vertraglich vereinbart. Das hat er so gemacht. Das ist nicht vertragsgemäß. Deshalb hat er einen Vertragsbruch begangen. Das wäre dann gut für mich als Anwalt, weil ich ihn dann direkt bei den Ohren packen kann. Deshalb achte ich immer darauf, dass alles sehr detailliert beschrieben wird.	Then in the worst case I could go to court and say, That is contractually agreed. That's what he did. That is not in agreement. That's why he started a breach of contract. That would then be good for me as a lawyer, because then I can grab him right by the ears. That's why I always make sure that everything is described in great detail.

I-8	Und dann kommt der Dienstleister und sagt, ja, also wir haben folgende Verschlüsselungsmaßnahmen etabliert und ergriffen, folgende Maßnahmen zur Pseudonymisierung, folgende Maßnahmen zur Belastbarkeit der informationstechnischen Systeme usw. Im Idealfall schreibt er mir dann zehn Seiten dazu und dann würde ich das sehen und sagen, okay, wow, das ist für mich schon mal justiziabel, weil da steht dann drin, er hat eine Verschlüsselung	And then the service provider comes and says, yes, so we have established and taken the following encryption measures, the following measures for pseudonymisation,he following measures for the resilience of the information technology systems, etc. Ideally, he would then write me ten pages about it and then I would see that and say, okay, wow, that's already justifiable for me.
I-8	Aber intern muss man es natürlich überprüfen, also ist man auch intern verpflichtet, seine Sache regelmäßig zu überprüfen, seine Arbeit regelmäßig zu überprüfen. Wenn etwas Neues eingeführt wurde, birgt es ein großes Risiko. Wir sollten uns das regelmäßig alle ein oder zwei Jahre ansehen. Und das wäre der wichtigste Punkt.	But internally, of course, you have to review it, so you are also internally obliged to review your thing regularly, to review your work on a regular basis. If something new has been introduced, it has a big risk. We should look at that regularly every one or two years. And that would be the main point.
I-5	wenn ich irgendwas Neues einführe dass wir haben schon irgendeine Tool, das funktioniert gut und die bringen was Neues raus, dass man das dann auch einsetzen möchte, dass man dann nochmal den ganzen Prozess durchführen muss.	Yes, that's also the point, that when I introduce something new, that we already have some tool that works well and they bring out something new, that they then also want to use, that you then have to go through the whole process again.
I-2	Also ich glaube die Schwammigkeit ist gewollt dabei, weil sie ermöglicht neue Konstellationen mitzufassen. Und das ist auch die einzige Möglichkeit, dass Technik und Recht auch wirklich im Einklang irgendwo bleiben können, dass eben bei Recht ist ja eigentlich ganz anders Technik, nicht sehr dynamisch, sondern eben langfristig.	I think the vagueness is intentional because it allows us to capture new constellations. And it is also the only way that technology and law can really stay somewhere in harmony because law is actually quite different, not very dynamic, but rather long-term. (I-2)

I-7	Also ich glaube die Schwammigkeit ist gewollt dabei, weil sie ermöglicht neue Konstellationen mitzufassen. Und das ist auch die einzige Möglichkeit, dass Technik und Recht auch wirklich im Einklang irgendwo bleiben können, dass eben bei Recht ist ja eigentlich ganz anders Technik, nicht sehr dynamisch, sondern eben langfristig.	The more it comes, the better it gets with the guidelines, with all the court decisions, with all the new court decisions that are out there. The more solid it gets, the better. There's a lack of court decisions for practical work. That's what really fills it in and where the lines are drawn. Yes, they are all important too, the court rulings that are then also lacking for the practical work. That's what really fills it in then and where the lines are drawn then. (I-7)
I-11	Mit der Anonymisierung und den Vorgaben für die Anonymisierung steht man eigentlich recht alleine da.	With anonymization and the specifications for anonymization, you're actually pretty much on your own.
I-5	Und das ist halt aber für viele ein großes Thema, Behandeln, Daten anonymisiert sind, wie das funktioniert und so weiter. Das ist auch alles, was durch Wissenschaftsaufsichtsbörden und so weiter erst erarbeitet werden muss. Und selbst jetzt nach fünf Jahren ist man sich da noch relativ unsicher in vielen Bereichen.	And that's just a big issue for a lot of people, how do we deal with anonymized data, how does that work, and so on. These are all things that have to be worked out by science and regulators and so on. And even now, after five years, there is still a lot of uncertainty in a lot of areas.
I-12	Da kann man mal gucken, also dieser Intro abschnitt aus 25 und 32, wo es immer darum geht, Art und Umfang der Verarbeitung dann was es immer kostet und stand der Technik diese Sachen müssen halt alle da rein fließen um Risiko irgendwie abbilden zu können auch da gibt es kein einheitliches vorgehen auch nicht innerhalb der Behörden das ist sehr schwierig da quasi vergleichbare Ergebnisse zu kriegen	When you look at Articles 25 and 32, you're looking at the nature and scope of the processing, the costs involved, and the current state of the art. All of these factors need to be considered in order to make an accurate risk assessment. However, there is no standard methodology, even among the authorities, which makes it difficult to have a consistent assessment.

I-6	Da kann man in gewissen Maß, das sind 32, dann so quasi Risikostufen, man könnte das klassifizieren. Aber du hast trotzdem noch die Herausforderung, dass das erst mal eine Behörde mitgehen muss.	Article 32 allows for some grading of risk levels, but the challenge is that regulatory approval is critical.
I-12	Ja, Wissenschaft und die Praxis unterscheiden sich immer stark.	Yet its interpretation in academia stands in stark contrast to its practical, official application.
I-3	Es gibt die den aktuellen Stand der Technik, Aktuellen Stand der Wissenschaft, Industriestandards, eingeführten Industriestandards Das ist der Tag, was man den Techi immer mal sagen muss. Das ist nicht derselbe.	There's current state of the art, current state of the science, industry standards, established industry standards. That's what you always must tell engineers. It's not the same thing.
I-12	Wir machen keine Sachen wie Homomorphic Encryption oder Differential Privacy. Weil das heißt, das ist kein State of the art in unserem Sinne.	We don't do things like homomorphic encryption or differential privacy. Because that means they are not state of the art in our sense.
I-12	Privacy-Enhancing Technologies sind in der Wissenschaft state of the art für uns völlig irrelevant. Es muss jemanden Systeme bauen, die am Markt verfügbar sind.	Privacy-Enhancing Technologies are currently state of the art mainly in academia, but not in privacy compliance practice. Someone has to build systems that are available in the marketplace.
I-12	Es muss ein Software-Haus geben, was sagt, okay, wir bauen jetzt mal eine Lösung, die wir auf den Markt bringen und die Leute benutzen können, die durchgetestet ist, die auch skaliert für große Unternehmen, für Riesendatensätze, für verschiedene Datenbanken.Und bevor solche Lösungen nicht auf den Markt verfügbar sind und auch ausgereift sind, spielt die für die behördliche Praxis, spielen sie leider keine Rolle.	Someone must build systems that scale for large enterprises, for big data, for different databases. And until those solutions are available and mature, unfortunately they don't play a role in government practice.

I-12	Also von behördlicher Seite ist mir nichts bekannt. Einfach auch, weil was manheute schreibt, kann übermorgen halt schon veraltet sein.	That's why I don't know anything about government. Just because what you write today may be obsolete the day after tomorrow.
I-4	Was ist das, was ist die Konsequenz von der Anwendung einer solchen Technik? Ja, und zwar nämlich auf Anwendbarkeit, von Datenschutzrecht, Anwendbarkeit von Verarbeitung	What is it, what is the consequence of using such a technology? Namely on the applicability of data protection law, the applicability of processing. processing.
I-12	Ich meine, wenn es auf dem Markt nicht verfügbar ist und nicht eingesetzt wird, wird sich auch kein Jurist hinstellen und sagen, ich beurteile das mal. Das ist halt schwierig, weil wir prüfen die Realwelt, Datenverarbeitung und wir können nur das prüfen, was halt eingesetzt wird und wenn es einemakademischen Prototypen-Konzept irgendwo liegt, kriegt das kein juristische Bewertung.	I mean, if it's not available on the market and it's not being used, no lawyer is going to stand up and say I'm going to evaluate it. It's difficult because we're testing the real world, computing, and we can only test what's being used, and if it's an academic prototype concept somewhere, it's not going to get a legal evaluation.
I-7	Das ist selber das Problem, dass wir auch in Beratungen auch immer haben. Man muss halt immer sagen, im Juristischen Bereich, das will niemand hören, aber es kommt halt immer auf den Einzelfall an,auf die konkrete Verarbeitung und dann muss man sich halt anschauen, ob es funktioniert oder nicht.	That's the problem we always have in consulting. You always have to say that nobody in the legal field wants to hear that, but it always depends on the individual case, on the specific processing, and then you have to see if it works or not.

I-12	Ja, aber auch das, da muss ich nochmal auch vorhin zurückkommen, das ist eine Einzelfallenentscheidung. Da muss ich mir ganz genau die Verarbeitungsvorgänge angucken, was für Daten werden verarbeitet, welche Dimensionen haben diese Datensätze und erst dann kann ich irgendwie eine Entscheidung darüber treffen, was für Technologie nicht mit welchen Attributen und Rahmenbedingungen dann einsetze.	Yes, but that too, I have to come back to that earlier, that is a case-by-case decision. I have to take a very close look at the processing operations, what kind of data is being processed, what are the dimensions of these data sets, and only then can I somehow make a decision about which technology not to use with which technology not to use with which attributes and under which conditions. and then use it.
I-6	. Es wird dir erheblich nicht erschwer, aber die Anforderungen, die Anforderungen extrem hoch und der Aufenthalte getrieben werde muss im Compliance-Zentrum, wird deutlich zunehmend werden.	The compliance requirements are going to increase significantly in terms of data. The demands, the requirements are extremely high, and the push in the compliance center will increase significantly.
I-6	Sie wollen so diesen Single-Market für Datenverarbeitung schaffen, aber halt einfach, dass der Datenraum in Europa freier Datenfluss ist.und Datenverkehr und so was. Also ganz klar das Recht formt den Bereich Daten.	They want to create this single market for data, but they also want the data space in Europe to facilitate the free flow of data and data traffic. So, it's clear that legislation is shaping the data space.
I-3	Das ist für mich als Anwalt, natürlich eine Herausforderung,weil das Voraussetzt, dass ich das kann, dass ich das verstehe. Also nicht die englische Sprache, sondern die technische Sprache Ja, das sind noch nicht die Regeln.	This is a challenge for me as a lawyer, of course, because it requires that I can do it, that I understand it. So, it's not the English language, but the technical language.
I-6	Der Begriff spielt praktisch keine Rolle.	The term [Privacy-Enhancing Technology] plays virtually no role in day-to-day work.
I-1	Es ist schwierig, den Begriff Datenschutztechnologien aus rechtlicher Sicht zu definieren. Es gibt keine Standarddefinition. Aber ja es ist ein weit gefasster Begriff.	It is difficult to define the term privacy technologies from a legal perspective because there is no standard definition. It is indeed a broad term.

I-5	Nennen wir es Hass-Liebe, ja. Also es ist natürlich so, dass die IT-Sicherheit auf der einen Seite Hand in Hand geht mit dem Datenschutz. Dass beide das gleiche erreichen wollen. Es gibt allerdings auch Fälle, wo sich beide völlig entgegenstehen.	Let's call it Hate-Love, yes. So it is of course the case thatIT security goes hand in hand with data protection. That both want to achieve the same thing. However, there are also cases where the two are completely opposed to each other.
I-6	Also es ist im Endeffekt wichtig und sinnvoll, also beides kombiniert, Das eine ohne das andere geht nicht oder eher gesagt, Datenschutz geht ohne IT-Sicherheit nicht, aber nicht in jedem Bereich. Also manchmal, aber eher seltener steht es sich auch entgegen.	In the end, it is important and makes sense to combine the two, one without the other is not possible. or rather, data protection is not possible without IT security, but not in every area. So sometimes, but rather more rarely, they also oppose each other.
I-3	Ich muss so viel verstehen, dass ich weiß, wenn ich Fragen stellen muss und dass ich damit auch um den Aufsichtbehörde sagen kann, ich verstehe Ihre Frage und ich weiß, wer sie beantworten kann und das hole ich jetzt zusammen. Ich muss nicht die Antwort selber nicht haben.	I need to understand enough so that I know when to ask questions and that I can use that to say to supervisors, I understand your question and I know who can answer it and I'm gathering it now. I don't have to know the answer myself.
I-11	Das wäre schon nicht schädlich. Nein, nicht schädlich, weiß ich nicht. Aber nicht wirklich realisierbar?Es ist realisierbar, die Frage ist eben mit welchen Ressourcen und kontinuierlich ist ja so ein schönes Wort, die regelmäßig. Also selbstverständlich haben wir dort einen kontinuierlichen Verbesserungsprozess. Die Frage ist tatsächlich, was heißt inkontinuierlich?	That would not be harmful. No, not harmful, I don't know. But not really feasible? It is feasible, but the question is with what resources, and continuous is such a nice word, regular. So of course, we have a continuous improvement process there. The question is, what does discontinuous mean?

I-6	Die haben null Bock von irgendeinem Juristen sich irgendwie Jura zu erklären lassen, also das interessiert ihn nicht. Also das ist so, die sitzen dann jetzt nicht da und sagen, voll spannend wir sind heute da, wollen was über Datenschutz recht lang, sondern die sagen, so das ist das Produkt, so muss das funktionieren, das brauchen wir, damit es funktioniert.	They don't want a lawyer to explain the law to them, they don't care. So that's the way it is, they don't sit there and say it's exciting, we're here today, it's about privacy, they say this is the product, this is how it has to be, we have to make it work so it works.
I-2	Dann ruft man nicht für mich an und sagt, hey, kann ich für 200 Euro die Stunde, die Juristischen Rat, dazu haben.Okay, das heißt es ist eigentlich eher besser möglich, wenn man vielleicht irgendwie in einem großen Unternehmen ist mit einem in-house legalen Team.	They don't call me up and say, "Hey, can I get legal advice for 200 euros an hour? ' Okay, that's more possible if you're maybe in a big company where there's an in-house legal department."
I-5	Also die größte Herausforderung ist vor allem auch in kleineren Unternehmen so die Arbeitsbelastung. Also bei einem auch selten eine Person für den Datenschutz vollständig tätig ist, sondern es macht dann 30 Prozent aus von deren Arbeitsleistung. Und die haben wir bald 150 Prozent zu tun und dann das ist ja schon schwierig. Da sehe ich die größten Probleme in dem Bereich.	The biggest challenge, especially in smaller companies, is the workload. It's rare that one person is completely responsible for privacy, but it's 30 percent of their workload. Soon it will be 150 percent, and that's difficult. That's where I see the biggest problems.
I-7	kleine mittlere Unternehmen, die tuen sich sehr schwer damit. Also das kommt dann kaum ran eigentlich in die Ecke und zu Sachen wie Homomorphic Encryption, Verschlüsselung. Wo das insgesamt noch in der Forschung eigentlich würde ich ja mal sagen, dass die Ressourcenaufwand ist halt viel zu groß und das machen halt die großen Silicon Valley Unternehmen	Small- and medium-sized enterprises, you, and I, have a very hard time there. So that then actually hardly and things like homomorphic encryption, encryption. Where it's still in the research stage, I would say the resources required are way too high, and that's what the big Silicon Valley companies are doing, but otherwise only the big ones. So only the big ones.

I-8	Klar, extern ist es für uns schon auch wichtig, beispielsweise mit der Wissenschaft zusammenzuarbeiten und selbst auch wissenschaftlich zuarbeiten in manchen Bereichen, weil wir uns hat das auch erarbeiten müssen, gerade bei neuen Techniken oder auch wenn wir mit Behörden streiten.	Of course, it is also important for us externally, for example, to cooperate with academia and to do some academic work ourselves in some areas, especially when it comes to new technologies or when we are dealing with public authorities.

I-4	Ich glaube, wenn es um das Wie geht, ist es glaube ich wahnsinnig wichtig, dass man sich irgendwie versucht, so gut wie möglich, dass überhaupt machbar ist im universitären Bereich und ich kenne ja genug und weiß, wie die Schwierigkeiten sozusagen sind. Aber desto mehr man sich aus seinem Silo raus bewegt, desto besser wird's. Das heißt also, wenn ihr es hinbekommt, diese Art Arbeiten zu schreiben, idealerweise tatsächlich, wir haben richtig Bereich zu übergreifen, richtig Studienfach übergreifen, dass man da Wirtschaftsinformatiker mit reinziehen, dass man da Juristen mit reinzieht, dass Volkswirte mit reinzieht, dass man das Statistiker mit reinzieht, desto mehr man da Schwarm know how mit rein gießt, desto besser wird es, weil diese ganzen Themen bisher durchs darunter gelitten haben, dass es halt die Techniker gab, die gesagt haben, doch das geht, das ist total gut, aber es ist halt auch eine Myriade von sehr komplizierten, ja, Krypto logischen Verfahren, die da eingesetzt wird und da springt die ganze Lust und halt schon ab. Und wenn es dann darum geht, zu sagen, wo ist in dem wirtschaftlichen Mehrwert betriebswirtschaftlich und volkswirtschaftlich von dieser Art, damit die zu gehen, da brauchst du dann halt Volkswerte für und die brauchen verlass bare Zahlen und die können wir ihnen halt momentan davon noch nicht liefern,das heißt, sie springen dann auch ganz schnell ab	Ideally, we need to cross disciplines, cross fields of study that you can get, that you get business information scientists involved, that you get lawyers involved, that you get economists involved, that you get statisticians involved, [. Because all these topics have suffered from the fact that there have been technicians who have said, yes, that's possible, that's totally good, but there's also a myriad of very complicated, yes, cryptological methods that are used [...], and that's where all the enthusiasm and just jumps off. And when it comes to saying where the economic added value is in terms of business administration and economic value of this kind, so that they can go, then you need people's values for that, and you need reliable figures, and we can't give them that now, so they jump off very quickly.

I-8	Du musst mit den Leuten reden, du musst auch echt ins Gespräch gehen und immer wieder sensibilisieren, auch erklären, dass das kein Selbstzweck ist.	The requirements, for example the GDPR requirements, lead to the fact that people look at privacy. You must talk to people; you have to really engage in the discussion and keep explaining that this is not an end in itself.
I-8	Das andere Extrem wäre also, wenn die Kollegen in einen solchen Schockzustand verfallen würden, dass überhaupt nichts passiert. Das wäre unglücklich. Und hier das richtige Maß zu finden, das ist, glaube ich, die ganz, ganz große Herausforderung dazwischen.	So, the other extreme would be if the colleagues were to go into such a state of shock that nothing happened at all. That would be unfortunate. And to find the right measure there, I think that is to the, the very, very greatest challenges between those.
I-8	Also ich glaube, ganz zentral jetzt auch im Vergleich zu der Tätigkeit an der Uni ist meine Tätigkeit wirklich enabler. Also im besten Sinne des Wortes, dass wir versuchen, eine Konvergenz herzustellen zwischen datenschutzrechtlichen Anforderungen und wirklich auch den dahinterstehenden	So, I think, quite centrally now, also in comparison to the activity at the university, my activity is really enabler. In the best sense of the word, we try to create a convergence between data protection requirements and the people behind them, which is what it's really all about, economically driven necessities.

I-11	Das stimmt, aber am Anfang ist es natürlich, gerade wenn man das erste Mal mit den Kollegen und Kolleginnen zusammenarbeitet, dann fühlt sich das natürlich schon so ein bisschen wie der Einschnitt oder die Limitierung der Kreativität, weil man sofort das Gefühl hat, dass um irgendwelche Governance oder Compliance-Anforderungen, die man ich glaube mittlerweile haben wir mit 90 Prozent der Kolleginnen und Kollegen aus den Entwicklungsbereichen wirklich ein gutes Zusammenarbeit geschaffen, wo wir auch eher wahrgenommen werden als wirklich Kollegen, die das unterstützen, die es supporten und nicht die jetzt irgendwie versuchen, Einschränkungen auch künstlich her vorzunehmen oder den Datenschützern wichtiger zu machen, als er ist.	In the beginning it's natural, especially when you're working with colleagues for the first time, then of course it already feels a bit like the cut or the limitation of creativity. [...] I believe that we have now created a really good working relationship with 90 percent of our colleagues from the development areas, where we are perceived as colleagues who really support this, who support it, and who do not somehow try to artificially emphasize restrictions or make data protection more important than it is.
I-8	Aber ja, es ist ein Lernprozess. Wir führen auch unglaublich viele Schulungen durch. Mindestens einmal im Monat haben wir eine zwei- bis dreistündige Schulung, in der wir die Dinge im Detail durchgehen.	But yes, it is a learning process. We also do an incredible amount of training. At least once a month, we have two to three hours of training where we go over things in detail.
I-8	den betroffenen Personen wirklich Datenschutz so verständlich zu machen, dass sie ein Verständnis dafür bekommen, dass ihre Daten ein Wert haben, dass es nichts anderes ist, wie der fünf Euro schein in Geldbeutel	It is important to make the people concerned really understand in such a way that they understand that their data has a value, that it is nothing more than the five-euro bill in their wallet.

I-9	Ja, ja, gerade wenn man eben Gesetze fordert, ist es ja eigentlich auch unerlässlich, dass sich die Gesellschaft damit auseinandersetzt, weil viel passiert durch die Diskussion und Streit, und wenn es aber letztlich niemanden interessiert oder wenn es niemand versteht, dann gibt es auch wenig stimmen, die das fordern, und dann. Passiert es halt auch dementsprechend langsam.	Yes, especially if you demand laws, it is actually also essential that society deals with it, because a lot happens through the discussion and dispute, and if ultimately no one is interested or if no one understands, then there are also few people who demand it, and then it happens slowly.
I-4	Wenn wir Datenschutzmanagementsysteme implementieren, dann spielt da genau dieser Aspekt privacy-by-design und privacy-by-default ein Riesen-Rolle, weil es eine, sagen wir mal so, der dankbarsten Geschichten ist, die du als Prävention im Vorfeld machen kannst.	When we implement privacy management systems, this aspect of privacy-by-design and privacy-by-default plays a big role because that's, let's say, one of the most thankful stories you can do upfront as prevention.
I-4	Aber, und das ist vielleicht wichtig, es gibt ja durchaus eine Professionalisierung auch im Datenschutz über die letzten 10, 15 Jahre Und da hat dieses Thema Datenschutzmanagement, also wirklich aktives Datenschutzmanagement, wahnsinnig viel Bedeutung erfahren.	But and this is perhaps important, there has been an operationalization in data protection in the last 10 or 15 years, and this issue of data protection management, of active data protection management, has become incredibly important.

I-4	Ja, ja, die Entwicklung geht dahin, dass Leute, die ich Unternehmen beibringen, die man verantwortlich bewusst mit Daten umgeht und das tust du halt, indem du das Thema und das ist fast wie jedes andere compliance thema auch letztendlich mit einem entsprechenden Management System und ob das jetzt ein Informationssicherheitsmanagement System oder ein Text compliance Management System ist oder sonst was es geht immer um das gleiche du versuchst so effektiv und so effizient wie möglich Anforderungen regulatorische oder gesetzliche Anforderungen umzusetzen und	I teach companies to be responsible and aware of data, and you do that by addressing the issue, and it's almost like any other compliance issue, ultimately with an appropriate management system, and whether it's an information security management system or a text compliance management system or whatever, it's always the same thing, you're trying to implement the regulatory or legal requirements as effectively and efficiently as possible. (I-4)
I-10	Also, jetzt so zum Beispiel, es gibt noch keine Kerndokumentation, die muss dann aufgebaut. Mit Managementsystem meine ich, dass Dokumentensystemen, was hinter dem Datenschutz steckt, das heißt, viele bedarf, ein kohärentes System auf die Beine zu stellen, dass so eine Datenschutzleitlinie entwirfst,, die ganze Grundlagen Dokumentation aufbaut. Und das alles in sich geschlossen als Dokumentsystem, das nennt man dann Managementsystem, Und das brauchst du dann am besten auch modular auf, damit das dann verzahnt werden kann. Weil eine Policy ist immer ein grundlangen Dokument, das in einem Unternehmen beschreibt, welchen Anforderungen sich das Unternehmen im Bereich des Datenschutzes unterwirft. Wir befolgen den Grundsatz Privacy by Design, Privacy by Default und so weiter.	By management system, I mean that document systems that are behind data protection, that is, many need to build a coherent system, which therefore designs a data protection policy, which builds all the basic documentation. And all of that, as a self-contained document system, is then called a management system. And it's best to build it in a modular way so that it can be linked together. And level 1 is called the privacy policy. [...] A policy is always a foundational document that describes the requirements that a company must meet in terms of privacy. We follow the principles of privacy by design, privacy by default, and so on.

I-10	Das heißt, dann kannst du dir zum Beispiel ein Kernprozess bauen, der sagt, bei neuen Produkten, die eingeführt werden, dann werden wir so und so auf diese Art und Weise diese Anforderung erfüllen	For example, you can develop a core process that says, when we launch new products, we're going to meet this requirement so and so.
I-5	Also rechtzeitige Einbindung ist Punkt Nummer eins von Juristen. Also wir haben hier über Prozesse, über Guidances geregelt, dass da eben klar ist, wer was übernimmt, wie die Abläufe sind und das erleichtert es auch schon.	Timely involvement is a top priority for legal professionals. We have processes and policies in place so it's clear who's responsible for what and what the processes are, which makes it easier.
I-10	Wenn Sie ein neues Produkt auf den Markt bringen wollen, ist es wichtig, alle Abteilungen in die Entwicklung des Produkts oder der Dienstleistung einzubeziehen. Und genau dort können Sie all diese Fragen verankern. Sie können sagen: Okay, wenn Ihr neues Produkt gebaut werden soll, dann gelten standardmäßig die folgenden Anforderungen. Das heißt, es muss so gebaut werden, dass es von Anfang an sauber ist.	If you're going to launch a new product, it's important to involve all departments in the development of the product or service. And that's where you can anchor all these issues. You can say, okay, if your new product is going to be built, then by default the following requirements apply. That is, it has to be built so that it's clean right from the start.
I-11	Wir achten da schon sehr drauf, dass wir bei Neuentwicklungen entsprechende Anforderungen mit abbilden. Auch da haben wir mittlerweile in unseren Entwicklungsprozessen wirklich Gates, wo wir sagen, also Privacy ist mittlerweile ein Thema gerade bei solchen Produkten, wo wir beispielsweise Kameras verwenden, wo wir einfach wirklich sagen, das ist ein Gate und wenn da nicht ein Privacy Haken dran ist, dann wird das Thema auch nicht freigegeben.	We place great emphasis on mapping the relevant requirements in new developments. We now have real gates in our development processes where we say that privacy is now an issue, especially in products where we use cameras, for example, where we simply say this is a gate and if there is no privacy check mark on it, then the output will not be released.

I-5	Also ich kann als Datenschutz kann ich ja nicht anfangen, irgendein IT-Sicherheitskonzept einzuführen, sondern das IT-Sicherheitskonzept muss von der IT kommen. Und da kann es natürlich möglich oder auch sinnvoll sein, gleich damit zu starten oder gleich ein Datenschutzaspekte mit einzubringen, also sagen, wenn ihr ein Berechtigungskonzept auflegt, dann sind folgende datenschutzrechtliche Grundsätze zu beachten und je nach Unternehmen, wenn ich das auf der Unternehmensbasis mache, auch gleich zu sagen, wie es im einzelnen Unternehmen datenschutzrechtlich aussieht. Das kann ich auch allgemeiner fassen und sagen, grundsätzlich sollte das Datenschutzrecht ja dann so und so und so aussehen und da eben die einzelnen Bereiche durchgehen, bei der IT-Sicherheit um und auch und dann ist gleich darüber einzuführen. Also es ist keine schlechte Idee da gleich zu sagen, es muss immer mit beachtet werden, weil sonst komme ich an den Punkt, den wir oft haben, es wird irgendein System oder Konzept oder sonstiges eingeführt und im Nachhinein ist es dann so, dass der Anschutz die Bremse reinwerfen muss und dann das ganz wieder umgestellt werden muss.	As a privacy officer, I can't just bring in any IT security policy; the IT security policy has to come from the IT department. And of course it may be possible or useful to start with that or to introduce data protection aspects right away, i.e. to say that the following data protection principles must be observed when creating an authorization concept and, depending on the company, if I do it at the company level, to say right away what the data protection situation is in the individual company. I can also summarize this more generally and say that, in principle, the privacy policy should look like this and go through the individual areas, IT security and so on, and then it should be implemented immediately. So it's not a bad idea to say right away that it always has to be taken into account, because otherwise I come to the point that we often have, where a system or a concept or something else is introduced and then Anschutz has to put on the brakes and the whole thing has to be changed again.

I-8	Und das ist auch das, was wir von unseren ISO-Kollegen immer mitbekommen sind. und sagen, hey, wir sitzen eigentlich im gleichen Boot. Und wenn ihr eine Verschlüsselungsmaßnahme braucht, und wir eine Verschlüsselungsmaßnahme brauchen, let's cooperate.	We hear that from our ISO colleagues all the time. And they say, hey, we're actually in the same boat. And if you need an encryption measure, and we need an encryption measure, let's work together.
I-7	Und natürlich wissen Sie jetzt viel mehr über Informationssicherheit. Sie müssen nicht alles selbst machen, aber Sie müssen die Audits durchführen, in den anderen Abteilungen oder Fachbereichen, um die Audits bewerten zu können, Was Sie tun, klingt gut und plausibel. Ich werde es jetzt abhaken.	And of course, you now know a lot more about information security. You don't have to do it all yourself, but you do have to do the audits, in the other departments or specialties to be able to evaluate the audits, What you are doing sounds good and plausible. I'm going to check it off now.
I-7	Audits, also Datenschutzbeauftragte mit der juristischen Hintergrund, die müssen jetzt ja keine Experten sein und der Informationssicherheit, aber sie müssen halt zumindest Audits machen. Die Meinung vertrete ich zumindest, sie müssen Audits machen im Informationssicherheitsbereich und über diese Audits dann halt auch die Kontrolle übernehmen in dem Bereich. Sie müssen selbst aber keine Experten sein. Also so kommt man dann schon wieder dazu, dass man die Bücke da auch ein Stück weit schließen kann.	Yes, so it has to be interdisciplinary. That's what I was alluding to a little bit with these audits, audits, so privacy officers with a legal background who don't have to be information security experts., but at least they have to do audits. At least, that's my opinion, they need to do audits in the area of information security and then use those audits to take control in that area. But they do not have to be experts themselves. So that's another way to close the gap a little bit.
I-3	Obwohl ein großer Bedarf an Normen und Zertifizierung besteht, gibt es noch einige Hindernisse, die in den Gesprächen deutlich wurden: Die Regulierungsbehörde sagt immer, dass Sie, die Industrie, die Industrienormen machen. Aber in der Praxis ist das noch lange nicht der Fall.	Although there is a great need for standards and certification, there are still several obstacles in the way, which became clear during the interviews: The regulator always says that you, the industry, make the industry standards. But in practice, this is still a long way off.

I-5	Das ist so ein Beispiel, was auch noch so die Frage ist, wie es denn kommt und wie es funktioniert. sind so Artikel 42 Zertifizierungen. Also das wäre gerade das, was man ja dauerhaft hofft, dass es irgendwann mal gibt. Aber gab es halt bisher auch noch nicht. Also das sind so Artikel, die definitiv den Nachbessern brauchen, was man auch sehr stark vermisst.	That's an example, which is also still the question of how it comes and how it works. so Article 42 certifications. So that would be exactly what you would always hope that there would be certifications at some point. But it is just not there yet. So these are articles that need improvement, which is also very much lacking.
I-4	Wir haben, jetzt stand heute, haben wir zum ersten Mal, hat die an der Ordnungsausschuss vor ein paar Wochen erstmals beschlossen die Kriterien für die Zertifizierungsinstitute, die dann darum, dass sie das Zertifizierungsverfahren annehmen. Also ich brauche ja jemanden, der eine Standard entwickelt und dann braucht er den, der diese Standard zertifiziert. Und für diese Zertifizierer gibt es jetzt Kriterien. Das heißt ich habe noch keinen Zertifizierer und ich habe auch keinen, der einen Standard entwickelt hat.	We have now, today, we have for the first time, has the regulatory committee a few weeks ago for the first time decided the criteria for the certification institutes, which then around that they accept the certification procedure. So, yes, I need someone to develop a standard, and then I need someone to certify that standard. And now there are criteria for these certifiers. So, I don't have a certifier yet, and I don't have anyone who has developed a standard.

A.3. Additional Sources

During this research addtional sources were found based on insights from the interviews. This literature surrounds, the identified challenges and solution strategies. A short overview of the references of the additional literature is provided:

References:

[9] [22] [36] [35] [33] [34] [18] [58] [50] [59] [60]

Chair of Software Engineering for Business Information Systems
Department of Computer Science
School of Computation, Information and Technology
Technical University of Munich

Disclaimer

Before we start the interview, I would like to mention that this interview will be recorded for subsequent transcription. The transcription itself and any findings within will be utilized for research purposes and for the eventual publication in a thesis and/or research paper. Any personally identifiable information will be anonymized, and the final results will be shared in the end. Could you please confirm your consent to these terms?

Questionnaire

Background
1. What is your position and role?
2. How many years of experience in this field and in the company do you have?
3. What is your understanding of data privacy compliance? What do you think about the demand of Privacy by Design for data privacy compliance?
4. What is your understanding of Privacy-Enhancing Technologies? What is their relationship with Privacy by Design?

Data Privacy Compliance
5. Can you describe the process of data privacy compliance in your company or with your clients, particularly in the process of implementation of *technical measures* for data privacy compliance?
   a. What is your role in this process?
   b. With whom do you interact in this process?

Data Privacy Compliance Sources
6. What sources do you use in the process of data privacy compliance, particularly when dealing with *technical measures*?
7. Do you use tools or automation in your daily role? In what way are they helpful?
8. Is educating yourself further on technical measures / PETs important to you?
   a. What exactly about PETs would be most important for you to know?
   b. In what form would further education be most effective for you on this topic?
9. Can you describe challenges or obstacles that you have faced in which a deeper technical knowledge would have been helpful?

Privacy and Technology and Law
10. Speaking more generally, where do you see the intersection of data privacy compliance and technology? In your opinion, do there exist gaps here?
11. Where at this intersection is the inclusion of legal expertise important?
12. How closely linked are IT-Security and privacy compliance, particularly from the perspective of your role?
   a. Can you give concrete examples where the former has influenced your work in the latter?
13. How would you judge the awareness of PETs amongst your peers?
14. Do you have guidelines or procedures to deal with PETs (or other privacy technologies) for data privacy compliance in your company?
   a. What exactly do these guidelines / procedures consist of?
   b. How helpful are they?
   c. What are the obstacles and challenges that are faced in the legal sector when PETs are used?
15. In what way, if any, can current laws be improved to account for the obstacles or inefficiencies that we have discussed?
   a. Is more technical input needed to facilitate this change?

Strategies
16. What strategies can be implemented to make data privacy compliance more efficient when PETs are used?
   a. How can legal experts be assisted?
   b. Would guidelines or checklists be helpful? Otherwise, what other tools would be best in your opinion?
   c. Can you draw on any experiences that led you to provide these answers?
17. In what way can your legal expertise be utilized to facilitate this improvement?
18. What other sources need to be leveraged to improve data privacy compliance? (authorities, academia, etc.)

Looking Forward
19. What are the primary incentives for legal experts to improve their knowledge about PETs and other technology-related factors for privacy compliance?
20. How will the dynamic between PETs and law continue to change? Do you foresee changes in regulation to include these kinds of technologies?
21. How have you seen your role / work change in recent years, and how will it continue to change?
22. Is there any aspect on this topic we may have missed?
23. Can you refer anyone who would also be able to contribute to this discussion?

List of Figures

List of Tables

Bibliography

[1] *New poll reveals 7 in 10 people want governments to regulate Big Tech over personal data fears*. https://www.amnesty.org/en/latest/press-release/2019/12/big-tech-privacy-poll-shows-people-worried/. Accessed: 2023-09-08. 2019.

[2] *The Problems of Internet Privacy and Big Tech Companies*. https://thesciencesurvey.com/news/2023/02/28/the-problems-of-internet-privacy-and-big-tech-companies/. Accessed: 2023-09-05.

[3] *Google agrees to $392 million settlement with 40 states over location tracking practices*. https://www.cnn.com/2022/11/14/tech/google-location-tracking-settlement. Accessed: 2023-09-08. 2022.

[4] *Google Agrees to $392 Million Privacy Settlement With 40 States*. https://www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html. Accessed: 2023-09-05.

[5] *Facebook vor Einigung im Prozess wegen Datenmissbrauchs*. https://www.spiegel.de/netzwelt/cambridge-analytica-skandal-facebook-vor-einigung-im-prozess-wegen-datenmissbrauchs-a-e3537fa4-42bd-4a92-8756-cb4470725dca. Accessed: 2023-09-05.

[6] A. Mantelero. "The future of data protection: Gold standard vs. global standard". In: *Computer Law & Security Review* 40 (2021), p. 105500.

[7] E. Parliament and C. of the European Union. *Regulation EU 2016/679 of the European Parliament and of the Council*. May 4, 2016. URL: https://data.europa.eu/eli/reg/2016/679/oj (visited on 09/05/2023).

[8] *Google Revenue: Statistics on Market Share, Growth, and Acquisitions (2023)*. https://www.enforcementtracker.com. Accessed: 2023-09-08. 2023.

[9] I. C. Office. *Privacy-Enhancing Technologies*. accessed, 5-09-2023. 2023. URL: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf.

[10] M. Altman, A. Cohen, K. Nissim, and A. Wood. "What a hybrid legal-technical analysis teaches us about privacy regulation: The case of singling out". In: *BUJ Sci. & Tech. L.* 27 (2021), p. 1.

[11] M. Iezzi. "The Evolving Path of "the Right to Be Left Alone"-When Privacy Meets Technology". In: *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE. 2021, pp. 225–234.

[12] M. Skousen. "The right to be left alone". In: *Ideas*. Vol. 5. 2002.

[13] L. Lessig. "Code is law". In: *Harvard magazine* 1 (2000), p. 2000.

[14] A. Cavoukian. "Privacy by design". In: (2009).

[15] *What is GDPR, the EU's new data protection law?* `https://gdpr.eu/what-is-gdpr/`. Accessed: 2023-09-06.

[16] G. G. Fuster. *The emergence of personal data protection as a fundamental right of the EU*. Vol. 16. Springer Science & Business, 2014, p. 169.

[17] C. J. Hoofnagle, B. Van Der Sloot, and F. Z. Borgesius. "The European Union general data protection regulation: what it is and what it means". In: *Information & Communications Technology Law* 28.1 (2019), pp. 69 –72.

[18] C. Michelakaki and S. B. Vale. "Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR". In: FPF: Future of Privacy Forum. 2023, pp. 1–6.

[19] N. Baloyi and P. Kotzé. "Guidelines for data privacy compliance: A focus on cyber-physical systems and internet of things". In: *Proceedings of the South African Institute of Computer Scientists and Information Technologists 2019*. 2019, pp. 1–12.

[20] K. F Passos. "Compliance with brazil's new data privacy legislation: What us companies need to know". In: *Compliance with Brazil's New Data Privacy Legislation: What US Companies Need to Know: F. Passos, Khyara*. [Sl]: SSRN, 2021.

[21] I. C. Office. *Privacy-Enhancing Technologies*. Tech. rep. Infomation Comissioner´s Office, June 2023.

[22] I. C. Office. *From Privacy to Partnership*. Tech. rep. The Royal Society, Jan. 2023.

[23] O. Klymenko, S. Meisenbacher, and F. Matthes. "Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance". In: *arXiv preprint arXiv:2306.15497* (2023).

[24] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh. "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges". In: *IEEE Internet of Things Journal* 6.2 (2018), pp. 2159–2187.

[25] S. Haney, A. Machanavajjhala, J. M. Abowd, M. Graham, M. Kutzbach, and L. Vilhuber. "Utility cost of formal privacy for releasing national employer-employee statistics". In: *Proceedings of the 2017 ACM International Conference on Management of Data*. 2017, pp. 1339–1354.

[26] K. Nissim, A. Bembenek, A. Wood, M. Bun, M. Gaboardi, U. Gasser, D. R. O'Brien, T. Steinke, and S. Vadhan. "Bridging the gap between computer science and legal approaches to privacy". In: *Harv. JL & Tech.* 31 (2017), p. 687.

[27] J. Holzel. "Differential Privacy and the GDPR". In: *Eur. Data Prot. L. Rev.* 5 (2019), p. 184.

[28] P. N. Otto and A. I. Antón. "Addressing legal requirements in requirements engineering". In: *15th IEEE international requirements engineering conference (RE 2007)*. IEEE. 2007, pp. 5–14.

[29] W. ël Hassan and L. Logrippo. "Requirements and compliance in legal systems: a logic approach". In: *2008 Requirements Engineering and Law*. IEEE. 2008, pp. 40–44.

[30] S. Agarwal, S. Steyskal, F. Antunovic, and S. Kirrane. "Legislative compliance assessment: framework, model and GDPR instantiation". In: *Privacy Technologies and Policy: 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers 6*. Springer. 2018, pp. 131–149.

[31] A. Tsohou, M. Magkos, H. Mouratidis, G. Chrysoloras, L. Piras, M. Pavlidis, J. Debussche, M. Rotoloni, and B. G.-N. Crespo. "Privacy, security, legal and technology acceptance requirements for a GDPR compliance platform". In: *Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5*. Springer. 2020, pp. 204–223.

[32] A. Bobkowska and M. Kowalska. "On efficient collaboration between lawyers and software engineers when transforming legal regulations to law-related requirements". In: *2010 2nd International Conference on Information Technology,(2010 ICIT)*. IEEE. 2010, pp. 105–109.

[33] *Standard Data Protection Model*. `https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/`. Accessed: 2023-09-08. 2023.

[34] *IT-Grundschutz-Kumpendium*. `https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html`. Accessed: 2023-09-08. 2023.

[35] U. NAtions. *The PET guide - UN Statsistics Division*. Tech. rep. OECD, Mar. 2023.

[36] OECD. *Emerging Privacy Enhancing Technologies*. Tech. rep. OECD, Mar. 2023.

[37] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman. "Systematic literature reviews in software engineering–a systematic literature review". In: *Information and software technology* 51.1 (2009), pp. 7–15.

[38] G. Hornung. "Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework". In: *Privacy and Security in the Digital Age*. Routledge, 2016, pp. 181–196.

[39] D. A. Makin and L. Ireland. "The secret life of PETs: A cross-sectional analysis of interest in privacy enhancing technologies". In: *Policing: An International Journal* 43.1 (2019), pp. 121–136.

[40] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz. "A taxonomy for privacy enhancing technologies". In: *Computers & Security* 53 (2015), pp. 1–17.

[41] L. Helminger and C. Rechberger. "Multi-party computation in the GDPR". In: *Privacy Symposium 2022: Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT)*. Springer. 2022, pp. 21–39.

[42] R. Howley and G. Pattni. "PRIVACY ENHANCING TECHNOLOGIES: AN EMPIRICAL STUDY INTO THEIR ADOPTION AND USAGE IN UK ORGANISATIONS". In: *Living, Working and Learning Beyond* (2008), p. 415.

[43] T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz. "The privacy policy landscape after the GDPR". In: *arXiv preprint arXiv:1809.08396* (2018).

[44] G. E. Marchant. *The growing gap between emerging technologies and the law*. Springer, 2011.

[45] E. J. Kindt. "The use of privacy enhancing technologies for biometric systems analysed from a legal perspective". In: *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Springer, 2009, pp. 134–145.

[46] V. Clarke, V. Braun, and N. Hayfield. "Thematic analysis". In: *Qualitative psychology: A practical guide to research methods* 3 (2015), pp. 222–248.

[47] *European data strategy*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en. Accessed: 2023-09-05.

[48] *European Data Governance Act*. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act. Accessed: 2023-09-05.

[49] *Digital service act*. https://www.bundesregierung.de/breg-de/suche/eu-regeln-online-plattformen-1829232. Accessed: 2023-09-01.

[50] ENISA. *Privacy and Data Protection by design - from policy to engineering*. Tech. rep. ENISA, 2015.

[51] en. 2023. URL: https://www.statista.com/statistics/1155852/legal-tech-market-revenue-worldwide/.

[52] *Legal Technology Market Size To Reach $45.73 Billion By 2030*. https://www.grandviewresearch.com/press-release/global-legal-technology-market. Accessed: 2023-09-05.

[53] N. Boltz, L. Sterz, C. Gerking, and O. Raabe. "A Model-Based Framework for Simplified Collaboration of Legal and Software Experts in Data Protection Assessments". In: *INFORMATIK 2022* (2022).

[54] M. Hildebrandt. *Law for computer scientists and other folk*. Oxford University Press, 2020.

[55] *IT-Recht*. https://www.uni-saarland.de/studium/angebot/weiterbildend/it-recht.html. Accessed: 2023-09-08. 2023.

[56] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti. "A survey on homomorphic encryption schemes: Theory and implementation". In: *ACM Computing Surveys (Csur)* 51.4 (2018), pp. 1–35.

[57] P. Drogkaris and M. Adamczyk. *Data Protection Engineering: From Theory to Practice*. 2022.

[58] I. C. Office. *Anonymisation: managing data protection risk code of practice*. Tech. rep. Information Comissioner's Office, 2023.

[59] Y. Lindell. "Secure multiparty computation". In: *Communications of the ACM* 64.1 (2020), pp. 86–96.

[60] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao. "A survey on federated learning". In: *Knowledge-Based Systems* 216 (2021), p. 106775.