SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY - INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Information Systems

On the Relationship Between Security and Privacy in the Context of Information Systems

Felix Thorwächter

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY - INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Information Systems

On the Relationship Between Security and Privacy in the Context of Information Systems

Über das Verhältnis zwischen Sicherheit und Datenschutz im Kontext von Informationssystemen

Author:	Felix Thorwächter
Supervisor:	Prof. Dr. Florian Matthes
Advisor:	Stephen Meisenbacher, M.Sc.
Submission Date:	15.09.2023

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

Munich, 15.09.2023 Felix Thorwächter

Abstract

In the age of big data, safeguarding personal data has become paramount to the responsible and trusted processing of information. Parallel to the discussion revolving around the power hidden behind data, rising concerns regarding the dangers of large-scale data processing have likewise taken the spotlight. At the center of this debate often arises the intertwined topics of security and privacy as the two main pillars of defense against breaches of personal information. Due to their nature, they often need clarification as their boundaries are still blurry. This misunderstanding can lead to ineffective security and privacy practices, resulting in increased risks to organizations and individuals.

To solve this, the question then becomes: What is the relationship between security and privacy?
Although this may be naively answered by citing the differing definitions of the two concepts - which is not as trivial due to privacy being quite challenging to define - the question begs a deeper investigation. Research has revealed that security is often conflated with privacy and vice versa. Nevertheless, while closely related, they are not the same; moreover, they cannot and should not be treated as such.

This thesis builds upon the hypothesis that the relationship between security and privacy depends on the specific topic: While there are synergies in some areas, they sometimes have conflicting requirements or no overlap at all.
The core of this thesis aims to paint a broad picture of the relationship between security and privacy in practice. Moreover, this thesis explores those areas of overlap and then further differentiates them between possible synergies and conflicts.

Going one step further, the relationship between security and privacy might place the two notions at odds. Powerful technologies, such as Privacy-Enhancing Technologies (PETs), boast strict privacy guarantees to the point where security measures may become obsolete based on the nature of the data in question.

Can this be the case in practice?
After answering this, these results may be used as a basis for further research, e.g., to further analyze which PETs might replace or support traditional information security measures. This could lead to more straightforward and cost-effective security and privacy practices, which in turn might enhance the protection of personal information and increase security and privacy in general.

Kurzfassung

Im Zeitalter von Big Data hat der Schutz von persönlichen Daten oberste Priorität für die verantwortungsvolle und vertrauenswürdige Verarbeitung von Informationen. Parallel zur Diskussion über die Möglichkeiten und die damit einhergehende Macht, die in Daten verborgen ist, sind auch zunehmend Bedenken hinsichtlich der Gefahren von hoch-skalierter Datenverarbeitung in den Mittelpunkt gerückt. Im Zentrum dieser Debatte tauchen oft die eng miteinander verbundenen Themen Sicherheit und Datenschutz als die beiden Grundpfeiler zum Schutz von persönlichen Informationen auf. Aufgrund ihrer Natur werden diese oft miteinander verwechselt, da ihre Grenzen immer noch sehr unscharf und undefiniert sind. Das kann zu Missverständnissen führen, welche wiederum zu ineffektiven Sicherheits- und Datenschutzpraktiken führen, und schließlich die Risiken für Organisationen und Einzelpersonen erhöhen.

Um dieses Problem zu beheben, stellt sich die Frage: Was ist die Beziehung zwischen Sicherheit und Datenschutz? Obwohl die Beantwortung dieser Frage zunächst naiv über den Vergleich der Definitionen von beiden Konzepten erfolgen könnte - was aufgrund der Komplexität von Datenschutz, nicht so trivial ist wie es scheint - ist eine tiefere Untersuchung nötig. Tatsächlich hat die Forschung in der Vergangenheit gezeigt, dass Sicherheit oft mit Datenschutz verwechselt wird, und umgekehrt. Obwohl sie eng miteinander verwandt sind, sind sie nicht dasselbe; darüber hinaus können und sollten sie nicht gleich behandelt werden.

Diese Bachelorarbeit beruht auf der Hypothese, dass die Beziehung zwischen Sicherheit und Datenschutz vom jeweiligen Kontext abhängt: Während es in einigen Bereichen Synergien gibt, haben sie manchmal widersprüchliche Anforderungen oder gar keine Überschneidungen.

Der Kern dieser Arbeit zielt darauf ab, ein breites und praxisnahes Bild der Beziehung zwischen Sicherheit und Datenschutz zeichnen. Darüber hinaus werden die Bereiche, in denen es Überschneidungen gibt, analysiert und zwischen möglichen Synergien und Konflikten differenziert. Darüber hinaus könnte die Beziehung zwischen Aspekten der Sicherheit und des Datenschutzes die beiden Konzepte miteinander in Konflikt bringen. Leistungsstarke Technologien wie Privacy-Enhancing Technologies (PETs) bieten strenge Datenschutzgarantien, bis zu dem Punkt, an dem Sicherheitsmaßnahmen aufgrund der Art der involvierten Daten obsolet werden könnten.

Ist dies tatsächlich auch in der Praxis der Fall? Nach Beantwortung dieser Frage können diese Ergebnisse als Grundlage für weitere Forschungen dienen, beispielsweise um genauer zu analysieren, in welchen Bereichen PETs möglicherweise herkömmliche Informationssicherheitsmaßnahmen ersetzen oder unterstützen könnten. Dies könnte zu einfacheren und kosteneffizienteren Sicherheits- und Datenschutzpraktiken führen, was wiederum den Schutz von persönlichen Daten erhöht und die Sicherheit sowie den Datenschutz im Allgemeinen verbessert.

Contents

Abstract iii

Kurzfassung iv

1. Introduction 1

2. Foundations 3
2.1. Security and Privacy in the Context of Information Systems . . . 3
2.2. ISO/IEC 2700X Standards . . . 4
2.3. Privacy-Enhancing Technology (PET) . . . 6

3. Related Work 8

4. Methodology 10
4.1. Research Questions . . . 10
4.2. General Approach . . . 11
4.3. Step One: Theoretical Relationship . . . 11
4.3.1. Systematic Literature Review . . . 11
4.3.2. Concept Map . . . 14
4.3.3. Feedback Workshop . . . 15
4.3.4. Expert Interviews . . . 15
4.4. Step Two: Best Practices . . . 17
4.4.1. Expert Discussion . . . 17
4.4.2. Decision Tree . . . 18
4.5. Step Three: PETs . . . 18

5. Relationship between Security and Privacy 20
5.1. Definitions . . . 20
5.1.1. Information Security . . . 20
5.1.2. Privacy . . . 21
5.2. Protection Goals . . . 28
5.2.1. CIA triad . . . 28
5.2.2. Confidentiality in detail . . . 29
5.2.3. "Privacy-specific" aspects . . . 29
5.3. Requirements . . . 30
5.3.1. Legal requirements . . . 30
5.3.2. Customer Requirements . . . 33

5.4. Frameworks . . . 34
5.4.1. International Organization for Standardization (ISO) . . . 34
5.4.2. American Institute of Certified Public Accountants (AICPA) . . . 36
5.4.3. National Institute of Standards and Technology (NIST) . . . 37
5.4.4. Other important frameworks . . . 38
5.5. Measures . . . 38
5.6. Versions of Concept Map . . . 39
5.7. General concept map . . . 42

6. Evaluation of ISO 27001 Controls **45**
6.1. Evaluation Method . . . 45
6.2. Intended Use of the Results . . . 49
6.3. Results of the Analysis . . . 49
6.3.1. Summary of the results . . . 61

7. Privacy-Enhancing Technology (PET) Assessment **62**
7.1. Treatment of possible conflicts . . . 62
7.2. Summary of the results . . . 63
7.3. List of PETs . . . 63
7.4. On the Relationship Between PETs and Security Measure . . . 64

8. Discussion **67**
8.1. Key findings . . . 67
8.1.1. Confidentiality Overlap . . . 67
8.1.2. Past and present evolution of requirements: Best practices . . . 67
8.1.3. Future evolution of requirements: Rising customer requirements . . . 68
8.1.4. Security Implications on Privacy . . . 68
8.1.5. Privacy handling in Practice . . . 69
8.1.6. Use of PETs as a solution to security . . . 70
8.2. Limitations and future work . . . 70

9. Conclusion **73**

A. General Addenda **76**
A.1. Interview Questionnaire . . . 77
A.2. Interview Translations . . . 78
A.3. Results of ISO control analysis . . . 82

List of Figures **92**

List of Tables **93**

Acronyms **94**

Bibliography **95**

1. Introduction

Due to the increasingly digitized world, more and more data is created, and an era of big data has started during the last decade. These data are exposed to a rising number of threats: being stolen, exposed, ransomed, falsified, or deleted. Therefore, safeguarding data and preventing breaches has become increasingly important. Also, governments noticed this transition to the digital age and started to regulate the growing demand for protection, e.g., with the General Data Protection Regulation (GDPR).

In particular, safeguarding personal data has become paramount to the responsible and trusted processing of information. Parallel to the discussion revolving around the power hidden behind data, rising concerns regarding the dangers of large-scale data processing have likewise taken the spotlight.

Here, the fields of information security and privacy come into play: two very closely related areas with seemingly similar goals: protection. Due to their nature, they often need clarification as their boundaries are very blurry. This misunderstanding can lead to ineffective security and privacy practices, unclear responsibilities, or ineffective measures, resulting in increased risks to organizations and individuals. That being said, more needs to be done to investigate their intersection.

The question then becomes: What are the definitions of security and privacy, and how are these concepts related in **theory**? (RQ1)
This is further split into smaller questions: What is security? How can we define privacy? Moreover, how do those two interact with each other?

Although these questions may be naively answered by citing the differing definitions of the two concepts - which is not as trivial due to privacy being quite difficult to define - the question begs a deeper investigation. In fact, past research has revealed that security is often conflated with privacy and vice versa. But while closely related, they are not the same; moreover, they cannot and should not be treated as such. Chapter 2 summarizes some of the current approaches for determining their relationship. While there are obvious relations, we still lack a comprehensive overview as current research often only focuses on small sections of their overlap.

The primary goal of this thesis is to investigate the intriguing and important relationship between security and privacy more thoroughly. Beginning with a literature review, first, the relationship in theory is evaluated and presented with the help of a concept map.

Due to the practical nature of the fields of security and privacy, our approach goes beyond that. Therefore, the first results are then enhanced and expanded to their intersection in practice by adding the perspective of experts in the industry. This is achieved by interviews as well as discussions in a feedback workshop. This second step is represented in the second research question: From the viewpoint of information security experts, how do the concepts

of security and privacy overlap **in practice**, and what are possible conflicting requirements or synergies? (RQ2)
This thesis builds upon the hypothesis that the relationship between security and privacy depends on the specific topic: While there are synergies in certain areas, they sometimes have conflicting requirements or no overlap at all. These synergies could be used to increase efficiency, e.g., by merging similar approaches into one process. However, the results arising from possible conflicts are more relevant to this discussion. One prominent example of this - outside the information systems domain - is the debate arising from the surveillance of public areas, which, on the one side, improves security while, on the other side, infringing privacy.

Therefore, our approach tries to identify these areas by introducing another novel approach: Investigating which privacy risks may arise from security measures. For a structured approach, we follow the ISO/IEC 2700X frameworks [1] and evaluate which impact their proposed information security controls could have on privacy.

Based on this evaluation, further questions come up that lead to the final part of the thesis. How can we solve those possible conflicts? Could a PET be used there? Going one step further, to what extent can **PETs** fulfill information security requirements to replace information security measures in certain areas? (RQ3) As our approach for this is rather general, this part of the thesis can become a starting point for further research, where the different PETs and use cases are investigated more deeply.

[1] To be precise, the ISO/IEC 27001 annex controls, which are the controls described in detail in ISO/IEC 27002, are evaluated.

2. Foundations

In the first section of this chapter, we delve into the foundational aspects of security and privacy by narrowing the scope to the context of information systems. The next section introduces the *ISO/IEC 2700X standards*, which form a big framework and play a central role in our thesis. The final section of this chapter gives a brief overview of *Privacy-Enhancing Technologies*.

2.1. Security and Privacy in the Context of Information Systems

One big part of the thesis is to answer in detail what security and privacy are. This is defined in the respective chapter 5.1.

For now, we will start with very general definitions of security and privacy and scope them to the context of information systems. The Oxford Advanced Learner's Dictionary defines *security* as "the activities involved in protecting a country, building or person against attack, danger, etc.", or more general as "protection against something bad that might happen in the future". [1]

Also, the Cambridge Dictionary keeps this very broad approach by describing *security* as "the state of being, or making safe, secure, free from danger etc." [2] This gives a big range of various fields where security plays an important role:

Intuitively, security is associated with protection from physical harm. This dimension itself involves various other topics like health concerns, safeguarding property, and so on. To mention a few other expressions of security: They range from social security (e.g., trust), financial security (e.g., stability), environmental security (e.g., sustainability), and national security (e.g., defense).

Another domain that digitalization introduced extends security to the cyberspace. IT security, information security, cybersecurity - there are many phrases with different definitions and slightly different focus, but they all address security in this new situation. [1]

In this thesis, we will focus on information security, also called information systems security (InfoSec). This involves the "protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document,

[1] While there are no official definitions, the practical differentiation that we advocate is the following: IT security is a subset of information security, which mainly focuses on protecting IT infrastructure and company networks. Extending the scope from one company to the internet while shifting the focus to the network side, we get cybersecurity. [3]

and counter such threats." [4]

The general definitions for Privacy, on the other hand, have a rather narrow scope:
The Cambridge Dictionary defines *privacy* as "the state of being away from other people's sight or interest". [2]

Also, the Oxford Advanced Learner's Dictionary contains this aspect in their definition by describing *privacy* as "the state of being alone and not watched or interrupted by other people" but extends this to "the state of being free from the attention of the public". [1]

These definitions are direct results of "The Right to Be Let Alone," one of the key elements that privacy includes. It was initially proposed as "The Right to Privacy" in 1890 by Warren and Brandeis, marking one of the first times that privacy was considered in the context of laws and being very influential on U.S. privacy legislation. Originally, the issue that their law review wanted to address was the development of photography, as well as the increasing popularity of gossip that resulted in "photographs and newspaper enterprise [...] invad[ing] the sacred precincts of private and domestic life". [5]

Because of these new emerging technologies and societal changes, the understanding of privacy also changed, which made it necessary to react and modify the law. Over the years, there have been many more technological advances that further sharpened our world, adding many more aspects to privacy. This has made it rather difficult to define what privacy contains nowadays.

In the later part of this thesis, we will go into more detail, not only about how this "right to be let alone" affects our current understanding of privacy, but we will also introduce other important aspects that privacy includes. This is done to find more inclusive definitions of privacy and its many rights.

With the rise of information systems, privacy, like security, has gained more and more relevance in a digital context. Information systems are a "set of applications, services, information technology assets, or other information-handling components". [6]

As it is a way too large field to cover in a bachelor's thesis, we will focus on the relationship between security and privacy in the context of information systems and thereby intentionally leave other aspects out of scope.

2.2. ISO/IEC 2700X Standards

Because of the complex nature of information security, many companies decide to follow already established approaches and best practices. Those are constantly being developed and documented in information security frameworks. This, of course, can be applied to the topic of privacy accordingly.

One of the most prominent information security frameworks was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). They standardized the framework within the ISO/IEC 2700X standards, which are followed in parts of this thesis.

These standards provide guidance to establish an Information Security Management System (ISMS) by offering a "comprehensive framework [...] to protect [...] data through robust policies and best practices" and specify "principles and practices that ensure organizations take appropriate measures. [...] From asset management and access control to incident response and business continuity, these standards provide detailed guidelines to help organizations secure their networks." [7]

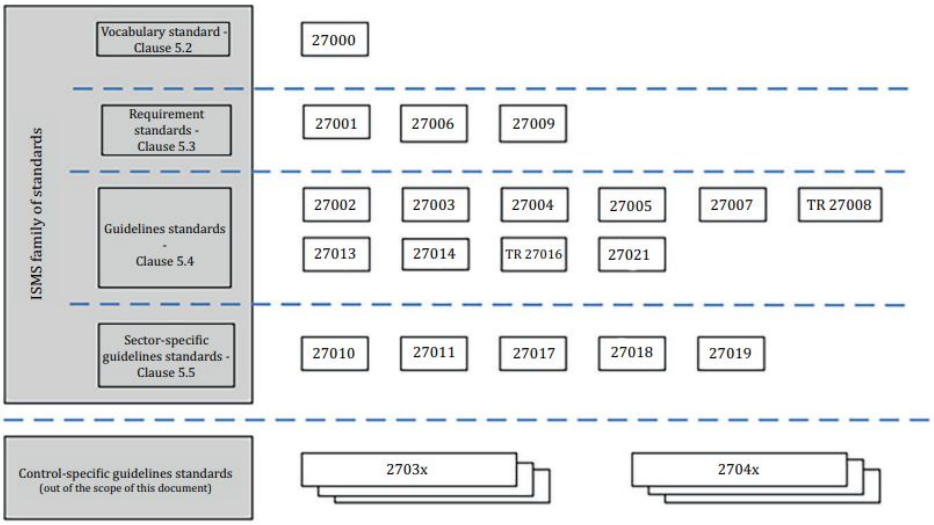

Figure 2.1.: ISO/IEC 2700X standards, adapted from ISO/IEC 27000. [6]

ISO/IEC 27000 describes the vocabulary and gives an overview of the other standards. Most relevant for this thesis are the following documents, which are summarized according to their official definition in ISO/IEC 27000 [6]:

ISO/IEC 27001 is the core document that "specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving formalized Information Security Management Systems".

Similar to other management systems (e.g., ISO/IEC 90001 or ISO/IEC 14001), companies can get ISO/IEC 27001 certified when they can successfully validate in an audit that they fulfill all requirements.

After describing controls and processes for the development and operation of the general ISMS, Annex A holds a "set of controls for the control and mitigation of the risks associated with the information assets".

Those "commonly accepted control objectives and best practice controls" are described more in detail in Sections 5 to 8 of **ISO/IEC 27002**. This document starts by describing its intended use by giving its scope, briefly summarizing used terms, definitions, and abbreviations, and explaining its structure. Following that, ISO/IEC 27002 describes the purpose,

specific advice, and best practice guidance for implementing the 93 controls. [6]

As one part of this thesis investigates the practical relationship between security and privacy, we decided to follow this framework to have a structured approach.

To increase clarity and readability while keeping precise, we will refer to the shared controls that are listed in Appendix A of ISO/IEC 27001 and described in detail in ISO/IEC 27002, simply as *ISO 27001 controls*. This is analog to the common referring to companies that have obtained certifications for this framework, as being ISO/IEC 27001 certified.

ISO also created a privacy-focused Privacy Information Management System (PIMS) that extends the ISMS, which is described in the ISO/IEC 2700X standards. This is formulated in ISO/IEC 27701 and includes privacy-specific controls, as well as additional guidance on how to implement ISO measures to ensure GDPR compliance.

As the ISO standards have a regular update pattern and are replaced by a new version every five years, the latest version of ISO/IEC 27701 is from 2019 and builds upon the version of ISO/IEC 27001 and ISO/IEC 27002 from 2017. [8] In 2022, the new versions of ISO/IEC 27001 and ISO/IEC 27002 were released. [9] This latest edition included some changes. While keeping most of the controls, their total number was reduced (from 114 controls to 93) as several old controls were merged or deleted while 11 new controls were added. The biggest change was the different structure and ordering of the controls, which also resulted in control identifiers. [2]

This forced us to decide which version to use in this thesis. We chose to use the latest 2022 edition, as there were some additions in the context of privacy; plus, in 2024, ISO/IEC 27701 will be updated.

2.3. Privacy-Enhancing Technology (PET)

With privacy legislation continuing to increase, more and better technical measures are needed to meet their requirements. While there is usually a technology-neutral approach in laws, like in the GDPR [10], PETs could be one solution to address this challenge: to fulfill privacy requirements. As implied by its term, PETs are technologies that enhance privacy. While this definition may be too broad, there is no official definition yet.

The Information Commissioner's Office describes

> "PETs [as] technologies that embody fundamental data protection principles by:
>
> - minimi[z]ing personal information use [...];
> - maximi[z]ing information security [3];

[2] For example, the control "Inventory of assets" moved from 8.1.1 to 5.9. While ISO/IEC 27002 includes a mapping, this additional step, when cross-working with documents referring to different versions and identifiers, increases complexity. Also, many of the controls were modified, so this mapping can only help to identify the references - the content to which they refer might have changed.

[3] In this context, *information security* is primarily used as a synonym to data confidentiality. We are discussing the

- or empowering people." [11]

There is a vast variety of PETs, each having different capabilities and features depending on their use cases. While all PETs provide privacy gains, the question is if they also increase security to a point where they might even replace traditional security measures.

One part of this thesis aims to find possible use cases for PETs by identifying areas where security requirements meet the need for privacy. In such areas where both security and privacy are important, maybe one solution that fulfills both might be utilized to use synergies by reducing the need for separate tools.

different aspects and protection goals of information security in chapter 5.1. Chapter 7 further addresses the use of PETs in the context of information security.

3. Related Work

One of the earliest descriptions of the relationship between security and privacy comes from James H. Moor (not to be confused with his namesake Gordon Moore, who made one of the most famous predictions in information technology).

He describes five different core values that are prominent in all societies – with security being one of them. Privacy, on the other side, is not, as it "has a distinctly cultural aspect which goes beyond the core values. Some cultures may value privacy and some may not." While the core values are commonly shared, their perceptions and expressions are still individual and depend on the cultural background; they are articulated in multiple different ways. This articulation is further called "expression of a core value". To put privacy in relation to security, Moor further proposes that privacy is "a natural expression of the need for security". This makes privacy one of many expressions of security, which can be interpreted as privacy being a subcategory of security. [12]

While this concise and elegant solution might have been sufficient in the pre-big-data age, nowadays, their relationship has become more complex and cannot be summarized in only a few sentences. One argument for that arises from the difficulty of describing what we understand under the two concepts of privacy and security. While information security is uniformly described, there are many different approaches to defining privacy. [13]

How these definitions look in detail is part of the first research question, which is why we will not go into detail at this place. Instead, we want to highlight that such complex fields have many different points of overlap, and their ambivalent relation in each of those is dependent on the topic. Therefore, we will consider this when analyzing the relation of both concepts and split this evaluation into multiple categories.

Another description of "[t]he symbiotic relationship between privacy and security in the context of the general data protection regulation" comes from Emanuele Ventrella. [14]
In this work, he further differentiates "the right to data protection from the right to privacy" on the grounds that the GDPR does not contain the word *privacy*. This differentiation is done for a similar reason to what we described in chapter 2.1; that our understanding of privacy has evolved and adapted to technological advancements of the digital world. In contrast to that, we still lack oversight over what privacy actually is, yet we have many guardrails like the GDPR in place to protect us.

In accordance with the title, his focus is on the context of the GDPR, while this thesis has a broader approach. While not only the security implications of article 32, the "Security of Processing" is analyzed, but also other parts of the GDPR are compared to their security implications. Our thesis also shifts the viewpoint by asking for the privacy implications starting from a security point of view.

One of the conclusions of this paper is similar to our goal to use synergies by having one solution that covers both security and privacy requirements. Ventrella describes this as "the employment of ICT solutions that—"by design"—integrate security measures implementing data protection safeguards [...] to ensure compliance with the obligations of the Regulation." [14]

We also want to mention the description of the differentiation between security and privacy from NIST here. In the Special Publication 800-53r5 [15], they describe the slightly different goals for protection that security and privacy have.

Security is relevant for "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized activity or system behavior) to provide confidentiality, integrity, and availability". [15]

Privacy is described as "managing risks to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal (collectively referred to as "processing") of PII and for ensuring compliance with applicable privacy requirements". [15]

The definition of security is very detailed and like our approach in chapter 5.1, but the definition of privacy feels broad and vague. It only focuses on an application of privacy, the management of Personal Identifying Information (PII), but does not specify what privacy is or which aspects it contains.

A different approach is taken in the NIST privacy framework, [16] represented in figure 3.1.

While the text mainly tries to reason that only managing security risks is not enough to also fulfill privacy needs, which serves as a well understandable introduction into the topic, [16] we strive for a deeper approach: not only using examples but rather explaining the backgrounds and goals of the different concepts. First, we also need to investigate the understanding of security, and in particular privacy. Also, we think that there are more overlaps, other than those related to "cybersecurity-related privacy events", like figure 3.1 suggests.

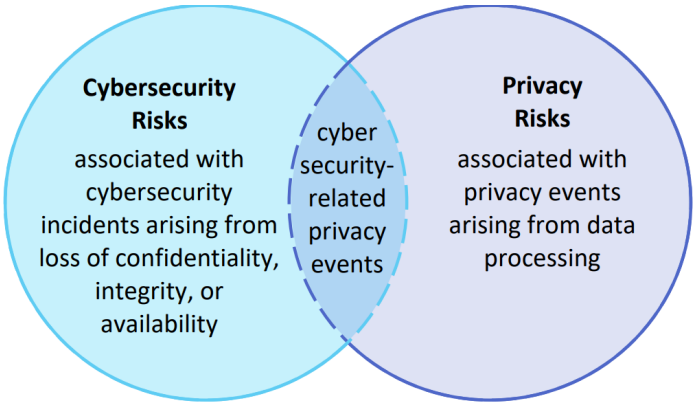

Figure 3.1.: Cybersecurity and Privacy Risk Relationship, adapted from the NIST privacy framework. [16]

This thesis tries to find further of those and gives more precise definitions for *privacy* Another approach of this thesis is to investigate if and how both concepts interact and influence each other. Focus on the possible impact that security controls have on privacy.

4. Methodology

This chapter discusses the methods used for creating this thesis. We will start by introducing the Research Questions, followed by an overview of the general approach.

4.1. Research Questions

This thesis aims to clarify the relationship between security and privacy in the context of information systems. To approach this broad field in a structured way, we will introduce the three research questions in this section.

RQ1: What are the definitions of security and privacy, and how are these concepts related in **theory**?

RQ2: From the viewpoint of information security experts, how do the concepts of security and privacy overlap **in practice**, and what are possible conflicting requirements or synergies?

RQ3: To what extent can **PETs** fulfill information security requirements to replace information security measures in certain areas?

The first research question establishes a foundation for the thesis by defining the concepts of security and privacy, as well as creating a fundamental understanding of the complex and multifaceted intersection by taking literature as input.

The second research question then expands these first results by adding first-hand from security experts. This way, we also have an added validation cycle and can focus on the most important aspects. Because this thesis builds upon the hypothesis that the relationship between security and privacy depends on the specific topic, the second part of RQ2 is to find out possible conflicting requirements or synergies. Our structured approach to getting comprehensive results is to follow a security control framework that outlines industry best practices. We analyze its proposed measures for their impact on privacy.

The third research question is to investigate if we can solve these discovered conflicts using PETs. Going one step further, the research will investigate if the use of PETs can replace the need for certain information security tools in areas where PETs also fulfill information security requirements. This could make security measures obsolete in those areas.

4.2. General Approach

We decided to divide the methodology section into multiple segments to match the mixed methods approach of this thesis. For each of the three key steps (see figure 4.1), we employed different data collection and analysis approaches. These methods are described in detail in each respective chapter to increase clarity, highlight the chronological progression of the results, and minimize potential confusion. The whole process is visualized in figure 4.2 at the end of this chapter.

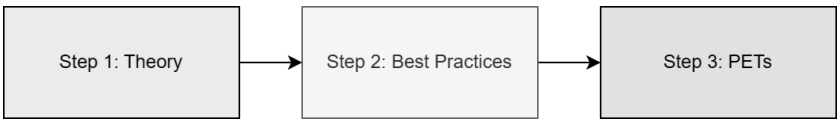

Figure 4.1.: The three key steps.

Before going into the specifics of the methods used in the initial step, we want to give a general overview of the whole data collection process:

The primary goal of the first step was to answer the first two research questions to comprehensively describe the relationship between security and privacy. For that, we conducted a systematic literature review and synthesized its results in a concept map. In addition to that, we held a small workshop with ten security experts to validate and improve the initial results. The third method used was conducting semi-structured interviews with security and privacy experts. These results were evaluated and used to further expand the concept map. The main part of the interviews focused on the content of this first research step, but some questions regarding the other parts of this research were included, as described below.

The second step focused on the measures. There, we deductively investigated the impact that security measures may have on privacy. For this qualitative analysis, we created a decision tree based on discussions with a security expert and the collected knowledge from the first step. The results of this analysis were then validated in the interviews.

The final and third step was interpreting the results from step two. Here, the question was addressed if PETs can solve the identified conflicts. Similar questions were part of the interview, so we could also include experts' opinions by summarizing their responses.

4.3. Step One: Theoretical Relationship

Having outlined the overview of our methods used, we can now delve into the detailed description of the methodology for step one.

4.3.1. Systematic Literature Review

First, a systematic literature review (SLR) was performed based on the guidelines proposed by Kitchenham and Charters. [17]

Research Questions

The first step of performing an SLR was to define the research questions that the SLR would answer. (5.3 in [17]) For that, we used the questions arising from RQ1 that we already introduced in the first section of this methodology chapter:
How are security and privacy defined?
In what areas and how are the two concepts of security and privacy related?

Search Strategy

For the selection of Databases, we started with scanning through some of the most prominent databases that are listed in table 4.1:

Database	**Domain**
ACM digital library	https://dl.acm.org/
Google Scholar	https://scholar.google.com/
IEEE Xplore	https://ieeexplore.ieee.org/
OPAC	https://www-ub-tum-de.eaccess.tum.edu/opac
ScienceDirect	https://www.sciencedirect.com/
Scopus	https://www.scopus.com/

Table 4.1.: Databases used

As most of the relevant results regarding privacy and security came from IEEE Xplore, we mainly used this database as our source for the SLR.

Another database that we used was Nautos (https://www.nautos.de/), as it contains standards and norms that were analyzed.

In addition to that, we included grey literature due to the constantly changing fields of security and privacy.

Our search strings included various combinations as well as singular and plural forms of the following keywords:

- information security
- security
- privacy
- information system
- definition
- standard
- framework
- regulation

An example of some of the search strings, including the number of results in the IEEE Xplore database, is listed in 4.2.

Search String	Number of results
information security	152548
privacy	65432
security AND privacy	45105
information security AND privacy	25349
information security AND privacy AND information systems	16176
information security AND privacy AND standards	2121
information security AND privacy AND standards AND information systems	1507

Table 4.2.: Number of results based on keywords

Inclusion and Exclusion Criteria (6.2 in [17])

We excluded papers that were neither in German nor English or not available in full text. Often, some papers were available in multiple languages (e.g., the ISO/IEC standards), so we chose to use the English version to ensure the use of the same phrases and wording as the authors.

As the goal of the systematic literature review is to generate a baseline for understanding the relationship between security and privacy, we were focusing on papers that either already address their intertwining nature or that give us a better understanding of what information security or privacy are in general.

In particular, we searched for papers that included definitions of privacy, e.g., in their foundation chapters, to find out the understanding of other scholars towards privacy. We started with the same approach for security but did not stick to this process, as security was always very similarly defined (See chapter 5).

We excluded papers that described specific implementations or measures in detail because the scope of this thesis is getting a general understanding. Therefore, when analyzing measures, the level of detail in ISO/IEC 27002 was sufficient.

A further exclusion criteria that we used was the scope of this thesis, which focuses on the context of information systems in general. There are many papers about privacy in the context of health-related data. Because there are special requirements that apply only to the health sector (e.g., HIPAA), we excluded most of them to not distort the general and overarching picture that we are providing.

Initially, we started with 85 literature sources, with 62 being white and 23 being grey literature. We did not include the number of papers that might have been relevant but were not accessible in full. The filtering process, which not only included the abstract screening but also included a brief first investigation of the texts, led to the exclusion of many papers, as described by the inclusion and exclusion criteria. This resulted in 48 academic literature sources selected. During the backward search, we could grow this number to 63.

We want to note here that due to the results, we could exclude further papers in the data synthesis step; the reason for that is described in chapter 5.1.2.

Data Synthesis

The collected data was initially sorted into a mind map, which then was formalized into a concept map. We also wanted to include attributes of a Venn diagram in the visual representation of the data, so we color-coded the different nodes. Privacy topics were in blue, security in red, and overlaps between both concepts in green. We also created a list of papers that were found, including their Bibtex information, to have an overview of our sources, where which usable data was found, and to get support in quoting that information.

The next section will introduce the properties of a concept map.

4.3.2. Concept Map

We decided on this form of visual knowledge codification according to Kudryavtsev and Gavrilova [18] because we wanted to provide not only an overview but also give information on the overarching relationship between the different areas. They also recommended a concept map for representing so-called "WHAT-knowledge". In the context of questions like "What is the relationship between entities?" [18], which is exactly what we wanted to answer, they highlighted using concept maps.

Kudryavtsev and Gavrilova refer to the paper about concept maps from Novak and Cañas [19], which we applied during the construction of this thesis.

First, we needed to "define the context", which was done by "construct[ing] a *Focus Question*". [19] We did orient on the SLR, as the concept map was used to represent and bundle its results. Those "*Focus Question[s]*" were, therefore, the same as described in section 4.3.1.

The next part was to "identify the key concepts", which then were ordered from general to specific ones. In our case we ended with five big categories, which then went into further detail. This resulted in the construction of a "*preliminary concept map*". [19]

With that being in place, we then added "cross-links" between the different domains. In order to have a better overview of these relations, we also created a version that excluded the details of each segment and referred to it as *general concept map*.

Novak and Cañas state that "a concept map is never finished", which makes multiple "revisions" necessary to create a "good concept map". We applied this approach, as the preliminary concept map only included results from the SLR. During the feedback workshop and expert interviews, we had multiple revisions and continued to incrementally improve the concept map.

We used the tools provided from *Draw.io* [1] for the construction of the concept map.

[1] URL: `https://app.diagrams.net/`

4.3.3. Feedback Workshop

After the initial results were visualized in a concept map, we had the opportunity to get some feedback from ten security experts, validate and extend our results, and discuss the other approaches of this thesis.

This was done in a 30-minute workshop that was held in person in the context of an internal information security summit. Even though the participants were all members of the same multi-brand company, we still argue that the diversity of this group of experts was high enough to avoid possible biases. This was not only due to the big differences in size and industry of the brands but also since multiple participants had just recently joined the company and therefore had even more varying opinions.

Participant	Role (* also ISO)	Brand Size (Employees)	Industry	(Main) Region
W-1	* Director Information Security	Large (> 500)	Build + Construct	USA
W-2	GRC Manager			
W-3	Corporate Information Security Officer	Holding of all other companies		
W-4	Security Architect			
W-5	* Team Lead Internal IT	Small (< 100))	Operate + Manage	Europe
W-6	* Team Lead Infrastructure and Security	Large (> 500)	Planning + Design	Europe
W-7	* Security Consultant	Small (< 100)	Digital Twin	Europe
W-8	* Global IT Security and Business Operations Manager	Large (> 500)	Planning + Design	Europe
W-9	Senior Corporate Security Engineer	Medium (100-500)	Planning + Design	USA
W-10	* Team Lead IT Network and Infrastructure	Medium (100-500)	Build + Construct	Europe

Table 4.3.: Workshop Participants

4.3.4. Expert Interviews

To validate the results from the literature review, as well as to gain further insights into the working world, security and privacy professionals were interviewed. These interviews were semi-structured, as participants had different touching points with security and privacy topics, depending on their position and role. Therefore, the semi-structured character allowed a deeper investigation into the interviewees' areas of expertise while keeping the duration of the whole interview reasonable.

The interviews were developed according to George [20]. This involved five steps that are described in the following.

Step 1: Set your goals and objectives

As already mentioned, the reason for the semi-structured interviews was to validate previous results and to further gain insights from the perspective of information security experts.

Step 2: Design your questions

For this step, we incorporated various principles from Gläser and Laudel to ensure a good quality of questions. The questions were open (4.2.3 in [21]) and the few dichotomous

questions always led to follow-up questions.

Also, the neutrality of the questions (4.2.4 in [21]) was enforced, and insinuating or suggestive questions were avoided. This approach was also represented by providing only a reduced form of the assembled interview guide in the form of a questionnaire to participants before the interview.

Questions were formulated as clearly as possible (4.2.5 in [21]) or additional information was provided if necessary. Examples of such questions were the ones regarding the concept map or the measure analysis.

Despite having multiple aspects of a question in the written questionnaire, all questions asked covered only one element (e.g., one separate question was asked for security and one for privacy aspects, while it is formulated as privacy/security in the questionnaire.). (4.2.6 in [21])

We also made several improvements to the interview guide, as Gläser and Laudel suggest in 4.3.3 [21]. Most of the changes were direct results of previous interviews, as we tried to iteratively include new findings and feedback and made updates to the concept map.

In the following, we will briefly summarize the content of the interview guide. The whole interview guide is appended to this thesis in A.1.

The questionnaire consisted of 6 chapters, starting with general introductory questions about the participants' backgrounds. The first topic-related questions were about the definitions of security and privacy. After partitioners gave their personal definitions, the definitions from the concept map were shown and then reviewed. Next, general questions about the relationship between the two areas were asked, including asking for examples. After that, first, the general representation of relationships in the concept map was discussed before going into detail. In this step, we collected a lot of feedback and could iteratively expand the concept map by adding topics like, e.g., the involvement of risk, a differentiation between measures and controls, and adding the business context with the scoping aspect. Next, we asked about the relevance and roles of privacy and security topics in the work of the participants. The following questions were about the evaluation of the ISO measures, including asking for real-world examples of conflicts and how those were solved. After that, the questions revolved around the topic of PETs, including a discussion about possible future development and RQ3. Finally, the insights were summarized, and participants had the opportunity to share further insights.

Step 3: Assemble your participants

For interviewees, we started contacting the experts who took part in the small workshop. In addition, we could also include further experts from other domains and businesses to increase diversity.

In total, we could conduct interviews with 6 participants from 4 different companies with a combined working experience of over 107 years. Interviewees I-1, I-2, and I-3 were from the same cooperation. Three interviewees also participated in the feedback workshop. Therefore, their corresponding code from table 4.3 is also stated in the first column of table 4.4:

Code	Role	Company Employees	Sector	(Main) Region	Work experience
I-1 / W3	Corporate Information Security Officer	5.000	AEC/O, Partly media and entertainment	USA and Europe	10-20 years
I-2 / W4	Security Architect				> 30 years
I-3	Security Manager				20-30 years
I-4 / W1	Info Security Director / ISO	500	AEC	USA	5-10 years
I-5	Data Protection Officer	5.000	Broadcasting	Germany	5-10 years
I-6	Project Owner and Lead Developer	> 50.000	Insurance and financial services	Europe	20-30 years

Table 4.4.: Interview Partners

Step 4: Decide on your medium

Two of the interviews were conducted in person; one interview was held via Discord, and the remaining interviews were held via Microsoft Teams.

Step 5: Conduct your interviews

Before the real interview started, we included steps like getting permission to record the interview, giving a short summary of the research and how the interviews fit into it, and confirming the anonymity and pseudonymization of the interviewees and their responses. (according to [21] 4.3.2)

To create a transcript, the audio of all interviews was recorded. After the interview, this was used to create a transcript, and then the recordings were deleted.

We used the responses from each feedback to further develop the concept map and have iterative steps for each interview.

The interview length varied between 42 minutes and 1 hour 6, bringing the total duration to about 5 hours and 10 minutes.

Because the interviews with I-1, I-5, and I-6 were held in German, we translated their quotes. The original can be found in the table included in A.2.

4.4. Step Two: Best Practices

The goal of this second step was to analyze security measures and evaluate their impact on privacy. We chose to follow the ISO/IEC 27001 framework because of its international reputation. The following two sections give a brief overview of the methodology that we developed in order to have a structured and consistent approach that we then used for this analysis. As parts of this process can also be seen as results, we choose to describe them in more detail in the results chapter 6.

4.4.1. Expert Discussion

Before creating a process to evaluate the possible impact of ISO 27001 controls on privacy, we wanted to gain an understanding of how companies are currently handling similar investigations. For that, we contacted and arranged a further discussion with security expert I-1 to find out how his company handles privacy in their ISMS. As the context of

privacy assessments was mainly project management, we also included some questions in the interview with I-6 and considered his feedback while developing our method, visualized with a decision tree.

4.4.2. Decision Tree

The idea was to create a sequential decision process, represented by a decision tree, to have a uniform process to analyze the possible impact that ISO 27001 controls have on privacy.

Therefore, here we briefly describe what a decision tree is and how it can be evaluated.

A simple decision tree starts from the top and consists of question-nodes, end-nodes, and labeled edges that are connected to each other. The nodes contain simple questions that - in a binary tree - can be answered in two different ways. A classic example would be a question that can be answered by *yes* or *no*. The connected edge, which includes the answer to the question-node, is then followed and either reaches another question-node, where the process is repeated, or an end-node. This end-node is the solution to this decision tree that ends the analysis.

In our case, these end-nodes contain four three scenarios: *likely no impact*, *possible synergies* [2], and *possible conflict*.

Please refer to chapter 6, where the construction and evaluation are described in more depth.

4.5. Step Three: PETs

The first approach of this chapter was to find solutions to the *possible conflicts* that the ISO control analysis revealed. By applying privacy techniques, e.g., pseudonymization or anonymization, some measures could restore privacy again. This approach turned security measures into technologies that enhance privacy, which shares the underlying idea of PETs. This way, we identified areas where the conflicts could be solved, partly solved, or not solved.

The second part focused more on actual PETs. First, we collected a list of different PETs. For that, we mainly combined the PETs described in the guidance from the Information Commissioner's Office [11], as well as the PETs collected and ranked by their prevalence according to Fantaye [22].

Then, we tried to apply those PETs to the ISO controls. As there was no formal method for this, this part of this thesis aims to raise awareness of the existence of PETs and encourages the unconventional mapping of privacy technologies to security measures.

The third part of this step was to discuss a thought experiment that was created during the interviews. It tries to investigate if security measures are still necessary when perfect privacy

[2]Which itself was further differentiated into already existing *synergies* and *synergies possible*, meaning that the process described in the control could easily be extended to privacy considerations.

is achieved. The results of this discussion were then synthesized and further applied to the topic of PETs to answer RQ3.

On the next page, the whole process is visualized in figure 4.2

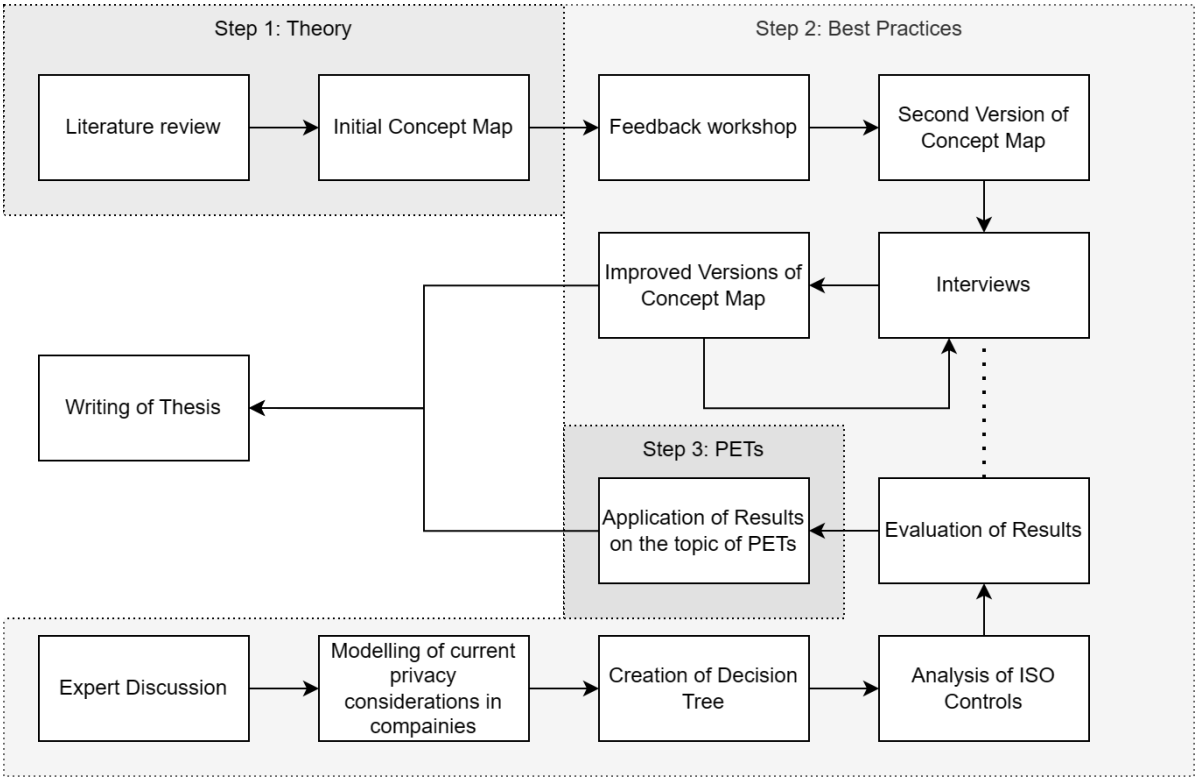

Figure 4.2.: Overview of the different steps during the creation of this thesis.

5. Relationship between Security and Privacy

This first results chapter aims to paint a broad and comprehensive picture of the relationship between security and privacy. Therefore, the following results are not exhaustive but rather focus on the most significant aspects of the topics.

In each of the following sections, we start by presenting the results of the SLR (4.3.1), in the following also referred to as *initial results*. These results were then verified and extended during the feedback workshop (4.3.3) and the expert interviews (4.3.4).

The results were visualized with a concept map. During the discussion of every topic, we will present a *detailed view* of the corresponding dimension of the concept map. The whole overview of the concept map, which we call *general view*, is shown and explained at the end of this chapter, in figure 5.11. Because we had different stages during the development of the concept map (see section 5.6), which also changed the *general view*, we will explain the relationship between the different dimensions at the end part of this chapter, in section 5.7.

5.1. Definitions

When it comes to evaluating the relationship between security and privacy, we first need to clarify their definitions. Figure 5.1 visualizes our findings.

5.1.1. Information Security

As all of the different approaches to defining security are very similar, we will work with the official definition from ISACA [1]:

Information Security "[e]nsures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)". [23] Those three protection goals (confidentiality, integrity, and availability) are also known as the CIA-triad and are described in detail in section 5.2.

This definition was also confirmed during the interviews:

- I-3 mentioned that the CIA triad was also part of the training during his certification as a CISSP (Certified Information Systems Security Professional).

[1] ISACA is short for the Information Systems Audit and Control Association, which is only using their acronym. They developed the COBIT Framework, which is mentioned in chapter 5.4. They also offer various internationally recognized certifications for IT professionals, for example, CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), or CDPSE (Certified Data Privacy Solutions Engineer). See `https://www.isaca.org/`

- I-2 added to this that security "involves proactive risk management, threat detection, and incident response to prevent, mitigate, or recover from breaches or attacks".
- I-1 also confirmed that "Confidentiality, Integrity, and Availability of data and systems" is an official definition.

With a clear definition of security, we can now delve into defining privacy.

5.1.2. Privacy

As privacy is very closely linked to the protection of Personal Identifying Information (PII), we first will describe in general what *PII* is.

Definition of PII

The GDPR [10] describes rules for the protection of *personal data*. By defining it as what we call *PII*, we are referring to the (*protection of PII*) as an important goal of privacy in this thesis, as the GDPR provides an accurate definition:

This includes "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". [10]

While this definition of data in scope differs between the legal frameworks, in the context of the GDPR, IP addresses are contained in this definition and are used in this thesis. [2]

Defining Privacy

With these foundations set, we can now start with defining *privacy*. In the following, we collected some definitions.

The ISACA glossary explains *privacy* as "[t]he rights of an individual to trust that others will appropriately and respectfully use, store, share, and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived". [23]

This definition contains two aspects of privacy: the *responsible use* and *purpose limitation* of data.

[2] For example, the California Consumer Privacy Act (CCPA) [24] talks about the protection of *personal information (PI)*, which is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes but is not limited to the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household". [24] Thereby, the scope is slightly shifted, as the CCPA specifically includes the protection of data from households, while the GDPR is on an individual level.

The International Association of Privacy Professionals (IAPP) [25] describes privacy "as perhaps the most significant consumer protection issue—if not citizen protection issue—in the global information economy." When it comes to defining *privacy*, they mention its many "widely differing views" and give some broad examples: "Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used. [...] Data privacy is focused on the use and governance of personal data — things like putting policies in place to ensure that consumers' personal information is being collected, shared and used in appropriate ways." [25] While this only includes some of the important aspects of *privacy*, the second part of this description highlights the bureaucratic parts of privacy.

This description supports our understanding of *privacy*, yet it is still very general and not specific enough to cover this concept in its many shades, which is what we are pursuing.

In the context of the Internet of Things (IoT), Lin et al. use the word *privacy* in two different contexts.

On the one side, it is listed as a "important security principle", to "ensure that the data can only be controlled by the corresponding user, and that no other user can access or process the data." [26] This is a very confusing use and needs to be carefully put apart to correctly understand its intention.

The first part mentions the control over data, which is indeed often described as an important privacy concept. The second part of the description points at the first glance to a security measure, more commonly known as access control. But, by adding the aspect of data processing, this goes one step further by not only prohibiting other users from accessing the corresponding user's data but also removing the systems - in this case, the IoT device - access to that data.

On the other side, there is a whole section describing privacy issues, as "a new challenge" that "can lead to property loss, and even compromise human safety" [26]. We will refer to this section in chapter 7, as their approach indirectly introduces different PETs.

Also, the interviewees defined *privacy* often in similar yet differing terms.

I-1 summarized: "*Privacy* is actually about protecting personal data. It means that my data should be protected the way I want it to be. Or the data of customers or individuals in general."

I-2 started with a less technical approach by describing *privacy* as "the state or condition of being free from unauthorized surveillance or intrusion into one's personal life or affairs." He then applied his definition to the digital domain by describing that *privacy* "involves the right to maintain and control information about oneself, preventing disclosure to others without consent".

I-3 defined privacy in the beginning mainly over its protection goals, which are discussed in detail in the next chapter (5.2). He then continued and described *privacy* as a collection of many questions: "Who has access to information? Who is authorized to [access] this information? [...] Who should have access to this information? What kind of information is

it? Is it classified? So, that [privacy] is mainly about granting access only to those people that should have it."

I-4 and I-5 mainly highlighted the compliance sides of privacy. I-5 summarized *privacy* as the "responsible handling of data" with a focus on "personal data and sensitive data".

I-6 added the principles of data minimization and the use of data only for "specific purposes". As a third aspect, he summarized that for him, having *privacy* means to remain "master of my data" by giving examples of rights regarding data deletion, right to information, and, like I-3, having control over the access to personal data.

Conceptualizing Privacy

As shown, there are many varying definitions that address several aspects of privacy. But they are either too narrow, by listing only examples, or too general. That problem was also identified by Daniel J. Solove. [13] He had similar results when using the common and most intuitive approach "to conceptualize privacy by isolating one or more common "essential" or "core" characteristics of privacy". Therefore, he successfully developed his new approach "by drawing from Ludwig Wittgenstein's notion of "family resemblances"". [13] [3]

Solove's approach resulted in six different *similarities*, or "conceptions", that are described in the following. While he tried to conceptualize privacy in general, we further applied his results mainly to the digital aspects of privacy.

1. The Right to Be Let Alone

This aspect is based on the *The Right to Privacy* from Warren and Brandeis [5], that was already introduced in chapter 2.1. The trigger was the merge of newspapers that harassed people by constantly taking photos and leaving no personal space.

To create legal boundaries to that, *The Right to Privacy* introduced a "rather broad and vague conception of privacy" by describing it "as a type of immunity or seclusion" and draws its justification from the Fourth Amendment. [4] [13]

Applied to the digital world, examples where this aspect is contained range from online harassment (like annoying newsletters or aggressive advertisement through pop-ups), social

[3] Wittgenstein described the idea of "family resemblances" in *Philosophische Untersuchungen* (*Philosophical Investigations* (PI)) in 1953. [27] He encountered the difficulty of defining *things* (like concepts) that are difficult to understand or describe. To state his point, he constructed a scenario in which the goal is to find a general definition for *games*, His first conclusion was that this was not possible, "we cannot give a final, essential definition of 'game,' so we cannot find "what is common to *all* these activities and what makes them into language or parts of language" (PI 65)" [28] Instead, we can extract "a complicated network of similarities overlapping and criss-crossing" (PI 66), which Wittgenstein described as "family resemblances". (PI67) We can use the (non-exclusive) "disjunction of all similarities" (PI67) to explain complex concepts like *games*, *numbers*, or in our case *privacy* are. [27, 28] In other words, "family resemblances" describes the relation between multiple *things*, which is not defined by one commonly shared feature, but rather through multiple overlapping *similarities* (of which not everyone has to apply for every*thing*).

[4] "The Fourth Amendment to the U.S. Constitution prevents the government from conducting "unreasonable searches and seizures." Government officials must obtain judicial approval before conducting a search through a warrant that is supported by probable cause." [29] With *The Right to Privacy*, the idea of this rule is applied to journalists, or in today's world also to social media.

media (analog to requiring consent before publishing pictures newsletters), and the use of cookies [5].

While we will focus in this thesis on personal information that can be described as PII, for the sake of completeness, we want to mention that also "being forced to hear propaganda, by being manipulated by subliminal advertisements, or by being disrupted" counts as an invasion of privacy. [13] [6]

To sum it up, this aspect is very self-explanatory: one must be let alone if asked for it.

2. Limited Access to the Self

This aspect, while similar to the right to be let alone, "is perhaps a more sophisticated formulation of that right." [13] It focuses on the *decision* "to what extent they [private information] shall be the subject of public observation and discussion." [32] It guarantees "the ability to shield oneself from unwanted access by others". [33] Yet Solove stresses, that this "is not equivalent to solitude. [...] Solitude is a component of limited-access conceptions as well as of the right-to-be-let-alone conception, but these theories extend far more broadly. [...] Limited-access conceptions recognize that privacy extends beyond merely being apart from others." [13]

Due to its origin from the same time as the *The Right to Privacy*, we need to transfer this to the information age.

As the *choice* of sharing *access* to personal data is at the center of the *Limited Access to the Self*, its main application is the demand of giving consent. Not only do smartphone apps ask for permission to use, e.g., the camera or the microphone, but also websites allow us to decide which privacy choices we have and store them in cookies. Another highly debated example is regarding making biometric identification systems mandatory. [7]

Because the choice granted by this conception of privacy is very individual, this aspect allows flexibility and considers the multiple different attitudes that people have towards privacy.

3. Secrecy

Perhaps the most common understanding of privacy is its *secrecy* aspect, which protects personal data against "public disclosure of previously concealed information". [13]

This description goes hand in hand with the definition of *confidentiality*, which is part of the security CIA triad. This overlap is investigated in more detail in chapter 5.2, as there remain differences between the security and the privacy sides of that conception.

[5] The use of certain types of cookies themselves could already be considered a violation to privacy. For multiple reasons, cookies are not banned but instead regulated to ensure privacy as they contain personal identifiers, thus counting as PII. [30] Yet these rules are sometimes breached, which results in fines. [31] Also, as cookies store privacy preferences, there has been a "proliferation of cookie consent pop-ups after it [the ePrivacy Directive] was passed" in 2009. [30]

[6] While Solove introduces these aspects that originate from DeCew in the context of criticism on the extent of *Control Over Personal Information*, which is described below, we already mention this here because we think this aspect is covered by the *The Right to Be Let Alone* perception of privacy.

[7] The topic of biometric identification systems is highly conflicting with security. Therefore, governments need to decide where to enforce such systems (e.g., mandatory fingerprints on digital passports) and where they draw the line (e.g., by regulating facial recognition in the EU to prevent mass surveillance). [34]

Also, *secrecy* in the context of privacy is sometimes interpreted as the "accessibility of information, not the mere secrecy of it". [13] [8]

Often, when we hear of *privacy* or *data breaches*, both aspects of *secrecy* are violated. Examples of this include the leak of private emails, personal health records, or credit card information.

The second interesting aspect of *secrecy* within privacy is often overlooked and breached when it comes to the extensive amount of profiling that many data-driven companies do (e.g., to perfect their targeted advertising). Aggregating data from multiple sources, including data brokers, may often lead to privacy violations because this data is "often collect[ed] [...] without the permission or awareness of the involved individuals." [36]

Summarized, the goal of *secrecy* in the context of privacy is to keep personal information secret and private while also considering the accessibility of these data.

4. Control Over Personal Information

This aspect is also closely related to the *Limited Access to the Self* but focuses not on the data collection but rather on the use and retention of them. Their relation is described that "control-over-information can be viewed as a subset of the limited access conception" [13]

That means that an individual still keeps "ownership in [their personal] information". While usually not intuitively connected to privacy, some researchers also view "intellectual property" as belonging to this category. This "is justified by viewing it [personal information] as an extension of personality." [13] This view comes with several other concerns, e.g., as relationships often influence such data, assigning ownership becomes difficult, or the problem of evaluating the "value of personal information for advertisers and marketers". [13]

As there are many different approaches to define *personal information* in this context, we mainly use the definition deriving from PII, which leads to several applications for the *Control Over Personal Information*.

As the legislative act Nr. 7 of the GDPR demands: "Natural persons should have control of their own personal data" [10], many of its components are driven by this conception of privacy. Being able to choose what personal data is collected, how this is used (purpose limitation), who has access, and with whom this access is shared are some of the rights following from this. The latter regulates companies that are selling user data, which is only allowed with the users' consent. [9]

[8] One example of this distinction was formulated by the U.S. Supreme Court in a case where "the release of FBI rap sheets (containing personal information from law enforcement records about millions of people)" [13] was rejected. The question was if these files, which "contain the history of arrests, charges, and dates that individuals have been incarcerated" [35], fall under personal data. On the one hand, such data themselves were considered as public data because "criminal information [...] was otherwise available in public records" [35]. On the other hand - which was the deciding factor - these data were only partly accessible, only at "one time or another", and the "bits of information" were "scattered". The judges concluded that releasing this information in a bundled way, therefore, would have violated privacy. [13, 35]

[9] Giving consent is usually part of either cookies or the terms of use, which are often written in ways that users either do not understand or that users are forced to accept to use the service or product. This way, the intentions of privacy protection are bypassed - sometimes unintentionally, sometimes deliberately. In the discussion chapter, we will talk about those problems regarding the handling of privacy in practice.

5. Personhood

This conception of privacy "differs from the theories discussed earlier because it is constructed around a normative end of privacy, namely the protection of the integrity of the personality" [13] *Personhood* can be understand of protecting "Individuality, Dignity, [...] Autonomy", and "Antitotalitarianism", why it is often rather associated to "liberty and autonomy than to privacy" [33]

Initially considered as a very general and vague description, that was also described in the context of abortion as "right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life" [37], this has become more prominent in the latest years with discussions around gender identity. [10]

Applied to digital privacy concerns, this conception aims to keep people's dignity by preventing, for example, intrusive profiling or stigmatization.

6. Intimacy

The *Intimacy* conception of privacy shifts the focus to "human relationships." [13]

With the focus on *intimate* information, all definitions that Solove gives could also be applied to the conception of *Secrecy*. The difference is the type of information that is protected: *Secrecy* focuses on "personal data" in general, *Intimacy* is about intimate and social "human relationships".

Therefore, we conclude that *Intimacy* is - freely speaking - the application of the *Secrecy* aspect on data which is about social relationships and the interactions among individuals. [11]

Examples of breaches are the eavesdropping of calls and private conversations, reading emails,

These findings are visualized in figure 5.1.

[10] Initially the *Personhood* argument was used after the state of Pennsylvania passed the *Abortion Control Act of 1982*. The argument was that the state should not breach the privacy of women by influencing their decisions in such personal matters. "In other words, the Court has conceptualized the protection of privacy as the state's noninterference in certain decisions that are essential to defining personhood" [13]

[11] Therefore, it could be argued that *Intimacy* should be a subcategory of *Secrecy*. As all conceptions are very closely related, we think this differentiation with *Intimacy* as its own conception makes sense due to its relevance and additionally due to the already complex definition of *Secrecy*.

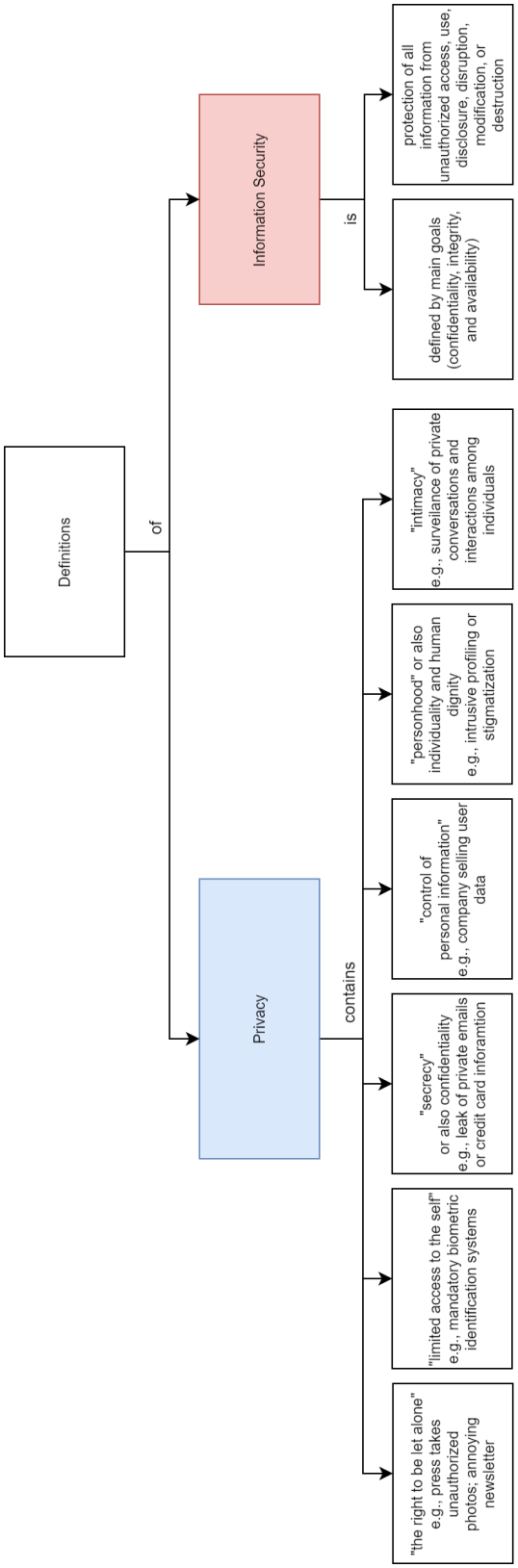

Figure 5.1.: Snapshot of the *definitions* dimension in the concept map.

5.2. Protection Goals

As discussed, security is mainly defined by its protection goals. Because the different conceptions of privacy formed several privacy principles that are summarized as an own protection goal.
In the following, we will go into detail what the different goals are. Thereby, we will focus on one important overlap while differentiating between the security and privacy sides of it.
In this figure, the conceptions of privacy principles are not contained, but they are linked to the *"privacy-specific" aspect* and represented in figure 5.4.

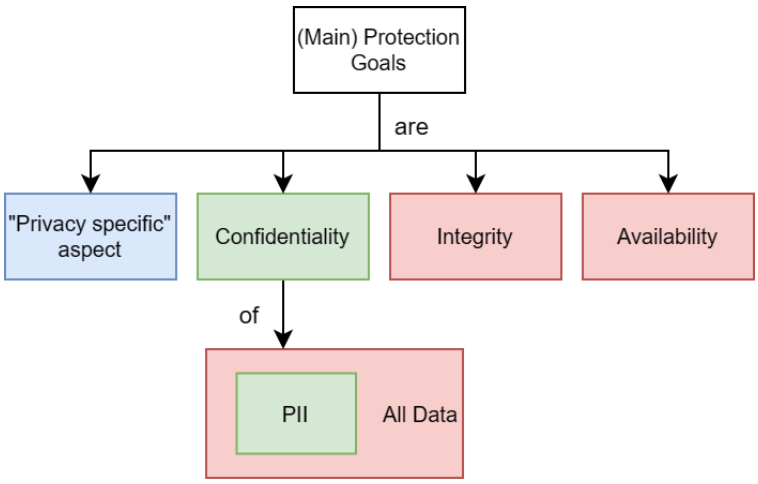

Figure 5.2.: Snapshot of the *protection goals* dimension in the concept map.

Figure 5.2 gives a visual overview. [12]

5.2.1. CIA triad

The CIA triad has already been mentioned. It consists of the three most important protection goals: confidentiality, integrity, and availability. [13]

In general, the three main goals are described in the following way:

- "*Confidentiality* means that information is not made available or disclosed to unauthorized individuals, entities, or processes" [38]
- "*Integrity* means accuracy and completeness of data and data processing methods" [38]
- "*Availability* means that information is accessible and usable upon demand by an authorized entity." [38]

Bertino [39] includes a deeper description and includes the relationship between security and privacy in this context:

"*confidentiality*, [as] referring to data protection from unauthorized accesses;
integrity, referring to data protection from unauthorized modifications;
and *availability*, referring to assuring that data be available to authorized users." [39]

[12] Security-specific aspects are color-coded in red, privacy-specific in blue, and overlaps in green.
[13] While there are also other goals that information security strives to achieve, which we will only mention here but not go into further detail: authenticity, accountability, non-repudiation, and reliability. [6]

She then lists *privacy* as a further "critical requirement". After mentioning the closeness between *privacy* and *confidentiality*, she then describes a relation between them:

"Data privacy requires ensuring data confidentiality because if data are not well protected against unauthorized accesses, privacy cannot be ensured. However, privacy has additional issues deriving from the need to take into account requirements from legal privacy regulations as well as individual privacy preferences." [39]

This results in two observations:
1. Privacy is dependent on security in terms of confidentiality, which marks one important overlap between both protection goals. [14].
2. Privacy has additional goals that go beyond security. Those are defined by both data privacy regulations as well as from the individual's perception of privacy. [15]

These observations are described in more detail in the next two sections and are already represented in figure 5.2.

5.2.2. Confidentiality in detail

Further papers mention this relationship in the *confidentiality* aspect between security and privacy as well. The security experts confirmed this relationship during the feedback workshop and the expert interviews. This demands a clear differentiation in this overlap.

For example the Systems and Organization Controls (SOC) frameworks developed from the AICPA, which will be introduced in section 5.4, give a good explanation: "Although confidentiality applies to various types of sensitive information, privacy applies only to personal information." [40]

Also the ISACA describes "that privacy refers only to information about people." [41]

To summarize: While information security is about protecting *all data*, privacy only focuses on *PII*. In this aspect, privacy is a subsection of information security.

5.2.3. "Privacy-specific" aspects

In general, we noticed that the word *privacy* is often used to describe not only the concept of privacy (which is on the same level as the concept of security) but also a protection goal (like confidentiality, integrity, or availability). To differentiate and to reduce semantic confusion [16], we called the latter *"privacy-specific" aspects*.

As we have discussed in chapter 5.1.2, there are many different perceptions of privacy, which leads to no universal definition of it. This, in turn, results in very blurry protection goals. Because only a few papers that talk about privacy also give definitions, we can only assume what the authors associate with privacy. Our approach is to combine the six different

[14] This privacy overlap is described in the next section *Confidentiality in detail*

[15] We named this second finding *"privacy-specific" aspects* in the concept map. They are deriving from the different privacy principles described in the next paragraphs.

[16] By comparing privacy to confidentiality, integrity, or availability, one might assume that privacy is on the same level and therefore considered as a protection goal, while it is, in fact, an overarching concept like security. Another example of this would be to compare *apples to vegetables*. The problem is the different abstraction levels of these words.

conceptions of privacy that Solove proposes and extends this to several of the most prominent privacy principles, which are described in chapter 5.4.

5.3. Requirements

After having defined what the goals of security and privacy are, we will discuss in the following what the different requirements to achieve these goals are and where they come from. [17]

Our initial solution mainly contained legal requirements, as the literature mainly features security and privacy compliance guidance. After the feedback workshop, it became quickly clear that there is a second group of stakeholders with raising demands. In the following subsections, we first name some of the most important legal requirements before delving into customers' requirements. The chapter after this will take a deeper dive into several frameworks. It could be argued that some of the legal requirements, like the GDPR, propose whole frameworks. But we kept them separated because regulations are more general about measures, while frameworks contain more specific ones.

5.3.1. Legal requirements

Security legislation

Starting with security requirements, we found that their regulations are mainly sector-specific. To use the precise juristic terminus, there are multiple *leges speciales* [18] , which addresses information security for certain sectors.

One example of such *lex specialis* is the **VAIT (Versicherungsaufsichtliche Anforderungen an die IT)** for insurance companies and the **BAIT (Bankaufsichtliche Anforderungen an die IT)** for banks. These regulations are from the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), the German Federal Financial Supervisory Authority. They contain several *minumum requirements* that companies in the corresponding sector must meet, or else they may be subject to regulatory action. [43]

I-2 confirmed this observation and mentioned one reason for that by bringing up an example from the automobile industry:

[17] We want to note again that this thesis includes just a small collection of the most important regulations that resulted from the SLR and the feedback that we got from the experts. To find a better overview of multiple other regulations, we suggest referring to the compliance offerings of international concerns. For example, Microsoft offers a good overview under `https://learn.microsoft.com/en-us/compliance/regulatory/offering-home`.

[18] A *lex specialis* (pl.: *leges speciales* are laws that are usually sector-specific. In contrast to them are the *lex generalis* (pl.: *leges genereales*), which are more general and universally apply. Jurists usually use this differentiation when multiple laws collide that are in a competitive relationship with each other. In these cases, often the "lex specialis derogat legi generali", the specific law overrules the more general one. [42] By using those phrases in this thesis, we do assume that there are no such conflicts and, therefore, do not make any assumptions on that *lex specialis rule*. Instead, we use the terms to improve clarity by using the general meaning of *lex specialis* to describe a *sector-specific law*.

"They [legal requirements] are there to protect the information [of the companies]. But they [the companies from different sectors] are doing it differently because of the different types of information that they're associated with. Banking is more associated with financial types of information, other than the loss of proprietary information from the automobile industry." E.g., the German automobile industry follows the **TISAX (Trusted Information Security Assessment Exchange)** mechanism, which is very strict on confidentiality topics. They are interested in protecting secret business information like the specifications of upcoming cars or the design of Erlkönige [19]. [44]

I-2 mentioned that these industry-specific regulations are necessary because while frameworks "like Network and Information Security Directive (NIS) or SOC 2 or the ISO 27001" are sufficient to create a "general" level of security, "for particular industries that's just not enough. There, you have to go a little bit more and beyond that."

We decided not to represent those specific rules in the concept map (figure 5.3) because its intention is to give a general overview. By leaving out the *leges speciales*, we only included one *lex generalis* for information security here, the upcoming second version of the **Network and Information Security Directive (NIS 2)**.

It can be argued that the first European **NIS Directive** from 2016 can be considered as a *lex generalis* as well. It is like a few months older German law regulating companies providing so-called "critical infrastructures", the BSI Critical Infrastructure Regulation (KRITIS). This was introduced in the scope of Germany's first IT Security law in 2015 (*IT-Sicherheitsgesetz 1.0*). [45] While it is overarching to multiple different sectors, it is still limited to only a few companies, the "critical infrastructures". While there have been additions to that, e.g., the *IT-Sicherheitsgesetz 2.0*, the scope has not really expanded.

The **NIS 2 Directive** will change this, as it immensely extends the range of its affected companies. [46] It affects 15 different sectors, including very big ones like manufacturing, food, or research. [47] By definition, this still counts as a sector-specific law, but due to its immense impact, we included it in the concept map.

I-1 also mentioned, that the "Cyber Resilience Act [...] will be a significant topic in 2026."

Privacy legislation

In contrast to information security, there are multiple *leges generales* for privacy. The most influential one within the European Union (EU) is the **General Data Protection Regulation (GDPR)**. It introduces several privacy principles that are explained in the context of the ISO frameworks in section 5.4. It did complement the ePrivacy Directive that was amended in 2009, which was also called "*cookie law.*" [48] While the initial plan was to update and release this in accordance to the GDPR as ePrivacy Regulation, "[t]he EU obviously missed that goal", but might be soon released. [30]

But also outside the EU are multiple privacy regulations. In California, we have, for example, the **California Consumer Privacy Act (CCPA)**, which was the "first comprehensive

[19] German car manufacturers use the term *Erlkönig* (pl. *Erlkönige*) to describe a disguised car prototype that is used for testing purposes.

[20] privacy law in the United States" when it was released in 2018. It gives consumers "General Data Protection Regulation (GDPR)-like rights", including the right to "'opt-out' for certain data transfers and an 'opt-in' requirement for minors." [CCPA subsection of [49]] Despite its more local application, during the feedback workshop, W-1, W-2, and W-9 noted that we should include these regulations, as their companies were affected by them.

Another privacy regulation in the US is the **Health Insurance Portability and Accountability Act (HIPAA)**. While HIPAA applies to the health industry - and therefore is sector-specific - we still included it in our list due to its relevance and its being one of the oldest privacy laws. Since it was introduced in 1996, technology has evolved a lot, and in 2009, its scope was extended with the Health Information Technology for Economic and Clinical Health (HITECH) Act. Its main goal is to protect sensitive health information by regulating their usage (compared to purpose limitations) and disclosure (confidentiality). [HIPAA and HITECH subsection of [49]]

The third and most recent important privacy regulation is the **Virginia Consumer Data Protection Act (VCDPA)** from 2023. It is "comprehensive privacy law" and incorporates rights like "providing disclosures, responding similarly to General Data Protection Regulation (GDPR) [21] consumer data subject requests [...], and complying with certain data processing obligations (for example, data minimization, [and] reasonable data security practices)". [VCDPA subsection of [49]]

Intergovernmental recommendations

We also included a third category here. While they are not binding laws but rather guidelines, we still sorted them under the *Regulatory Compliance* category, as they were released by intergovernmental organizations. The Organisation for Economic Co-operation and Development (OECD) adopted their **OECD "Recommendation on Cross-Border Co-operation"** in 2007. They include several privacy principles, namely collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. [50]

Also, the Asia-Pacific Economic Cooperation (APEC) proposed the **APEC Cross Border Privacy Rules System (APEC CBPR)** in 2011, which is "a voluntary accountability-based scheme to facilitate privacy-respecting personal information flows among APEC economies" [51] Within this, they also introduced the process to get systems certified as APEC CBPR compliant, necessary bodies, assessment criteria, and "arrangements for enforcing CBPR system requirements". [51]

The United Nations (UN) also highlighted the importance of privacy and proposed "**[t]he right to privacy in the digital age**" in 2013. The resolution highlights the importance of transparency, accountability, and oversight and demands that surveillance measures comply with international human rights law. They also called for action that the member states

[20] *Comprehensiv* means that this is a *lex generalis*.

[21] Yet the VCDPA has several differences to the GDPR. Some similarities, other than this transparency aspect, include the "[c]onsumer rights to access, delete, and correct their personal data." [VCDPA subsection of [49]]

should review and, if necessary, modify their laws and practices regarding surveillance and interception of communication. [52]

5.3.2. Customer Requirements

As already mentioned, companies can get their implementation of certain frameworks certified when they can successfully validate in an audit that they fulfill all of its requirements. In the following, we will discuss the benefits of such certifications, first from the customers' point of view and then from the perspective of the company or seller.

In some cases, it is mandated by *Legal requirements* that security or privacy controls are also met by their suppliers, for example if the customer is affected by NIS 2.0 [22] or KRITIS. Also, some controls of frameworks that are introduced in the next section handle privacy, or "[i]nformation security in supplier relationships". [9] That means, if the customer's company strives for such certification, they need to fulfill those controls related to their suppliers. To ensure compliance, it is often easier to rely on the certifications of those suppliers than to validate compliance with each control individually. Therefore, many customers nowadays ask for such certifications before signing deals, according to I-4.

I-4 also mentioned that their "sales department gets several security-related questions every week", which would result in a lot of work if they had to answer them individually. Therefore, they have prepared many "template[s] that answer most of the inquiries that [are] hand[ed] to customers on request." For big customers that request even further information, individual meetings are arranged, but a non-disclosure agreement (NDA) is required first "[t]o not jeopardize [their] security" [23]. "Having SOC [2] or ISO certifications would be an additional help", as they "could just refer to them." [24] These certifications are a good way to prove to customers that the company protects their data without revealing specific security measures.

While during the feedback workshop, the discussion around customer requirements was mainly security-focused, during the interviews also, a privacy requirement was mentioned. This customer requirement regards the geographical processing of data. I-4 mentioned that some European customers demand that data is being processed "within the European Union." This could be due to the different data protection laws, e.g., in the US, the government is allowed to "intercept [...] communication and deliver intercepted communication to" governmental agencies, which in turn are legally allowed to encrypt this data. [53] Figure 5.3 visualizes these findings.

[22] Even tough NIS 2.0 is still being adopted and not final, this is almost guaranteed, that it will be applicable for further companies than KRITIS currently involves.

[23] This was explained in more detail by I-4: This is "[f]or security reasons: If it is known that we use certain tools and systems and then there is a vulnerability found for that – or in the worst case a zero-day exploit exists – that could make us a target. We try to minimize our exposure – including what we communicate. You can say that we enforce the need-to-know principles also when dealing with customer relations."

[24] For this reason, the company of I-4 is currently in the certification phase of those two frameworks.

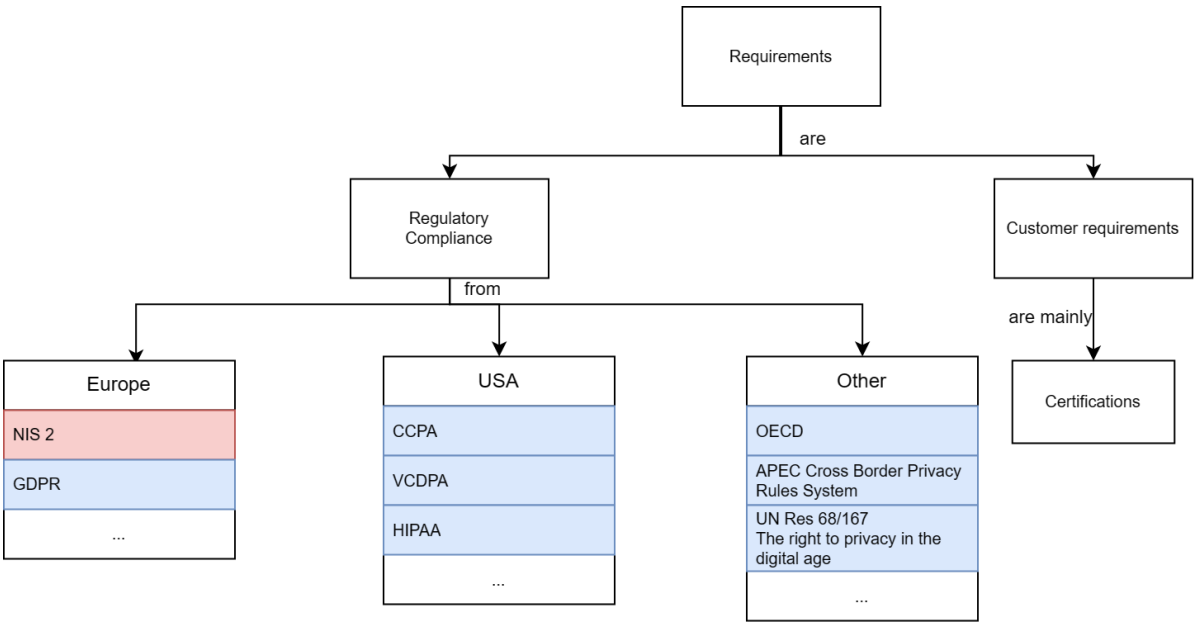

Figure 5.3.: Snapshot of the *requirements* dimension in the concept map.

5.4. Frameworks

As already introduced in section 2.2 of the foundations chapter, many companies decide to build their information security and privacy on internationally accepted frameworks. There are multiple reasons for that, which we will not go into detail here; instead, we want to give an overview of some of the most relevant ones. We ordered the frameworks from the organization that developed them. We also want to mention that there are mappings between most frameworks available.

Figure 5.4 visualizes the findings that are described in the following sections. We choose to expand two of the privacy principles here, as they are closely related to the *"privacy-specific" protection goal* described in section 5.2. Because some of the privacy principles overlap, we wanted to represent this in figure 5.4 by ordering them in a way that similar principles are at the same level. Because a deeper analysis was out of the scope of this thesis, we want to mention that this is only the draft resulting from a very brief analysis and could, therefore, not represent the actual overlap between these privacy principles. A more in-depth analysis is recommended before using our visualization.

5.4.1. ISO

The ISO/IEC 2700X framework was already introduced in section 2.2. It is one of the most prominent information security frameworks and offers certifications to companies complying with it. The security framework contains 96 controls that give guidance on the implementation of an ISMS. [7]

This framework can be extended to become a PIMS to ensure GDPR compliance. This is

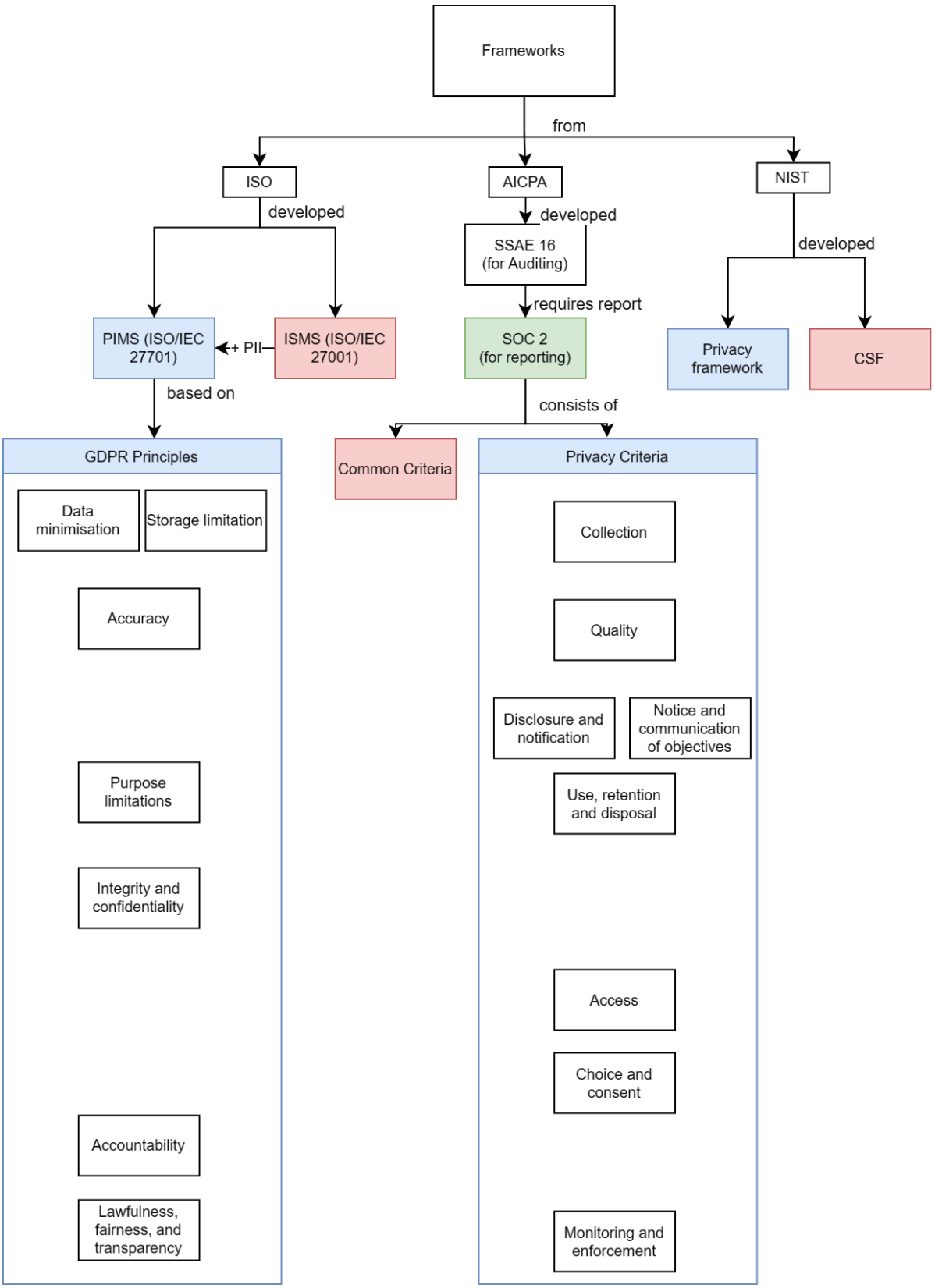

Figure 5.4.: Snapshot of the *frameworks* dimension in the concept map.

described in the ISO/IEC 27701 framework. Also, further frameworks like "ISO/IEC 29100 provide a high-level framework for the protection of PII within ICT systems". [9]

We will not go into detail about this but rather introduce the different privacy principles of the GDPR, as the ISO standard is very closely linked to it. Those are:

- Lawfulness, fairness, and transparency: PII is "processed lawfully, fairly and in a transparent manner in relation to the data subject". [10]
- Purpose limitation: PII is "collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall [...] not be considered to be incompatible with the initial purposes". [10]
- Data minimization: PII is "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed". [10]
- Accuracy: PII is "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". [10]
- Storage limitation: PII is "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to the implementation of the appropriate technical and organi[z]ational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ". [10]
- Integrity and confidentiality: PII is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthori[z]ed or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organi[z]ational measures". [10]
- Accountability: "The controller shall be responsible for, and be able to demonstrate compliance with" the other privacy principles. [10]

5.4.2. AICPA

W-1 and W-2 proposed during the feedback workshop that we should also add the framework around SOC 2. [25]

"SOC 2 is a security framework that specifies how organizations should protect customer data from unauthorized access, security incidents, and other vulnerabilities." [54] But as it

[25]While we tried to inform us, we noticed that our license did not contain access to most of the documents of this standard. Therefore, our results regarding SOC 2 are from secondary literature only, except the GAPP.

contains "controls [...] relevant to security, availability, processing integrity, confidentiality, or privacy" [55], we classify it also as a privacy framework, making it fall under the category of both. [26] Those five Trust Services Criteria (Security, Availability, Confidentiality, Processing Integrity, and Privacy) are then further differentiated. The "cybersecurity risk management reporting framework" [55], which includes several security principles, are referred to as *Common Criteria*. The privacy criteria "looks at how an organization's control activities protect customers' personally identifiable information (PII). It also ensures that a system that uses personal data complies with the AICPA's Generally Accepted Privacy Principles" (GAPP). [54] A company complying with these rules can be certified.

We will list the privacy criteria, that is based on the GAPP in the following:

- Notice and communication of objectives: "The entity provides notice to data subjects about its objectives related to privacy" [40]
- Choice and consent: "The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects." [40]
- Collection: "The entity collects personal information to meet its objectives related to privacy." [40]
- Use, retention, and disposal: "The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy." [40]
- Access: "The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy." [40]
- Disclosure and notification: "The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy." [40]
- Quality: "The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy." [40]
- Monitoring and enforcement: "The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes." [40]

5.4.3. NIST

The NIST has created several frameworks. Their most important ones are their Cybersecurity Framework (CSF) and the NIST Privacy Framework [16]. Also, a combination of both security

[26] We noticed, that in the context of SOC, the word *security* includes *privacy*, which makes this topic very easy to misunderstand.

and privacy, the NIST Special Publication 800-53, which includes Security and Privacy Controls for Information Systems and Organizations, has to be mentioned here. [15] [27] [7]

They provide a very detailed framework that integrates privacy and security controls, and they include a mapping to many other important frameworks.

5.4.4. Other important frameworks

This includes a small list of further important frameworks. Security frameworks are, according to Ryerse [7], and privacy frameworks to Prozorov [56].

- CIS Control Framework (security)
- PCI-DSS (security)
- ISACA Cobit Framework (security)
- ICO Accountability Framework (privacy)
- TrustArc-Nymity Integrated Privacy Frameworks (privacy)
- MITRE Privacy Maturity Model (and other Privacy Engineering Tools) (privacy)

5.5. Measures

Before starting with this section, we want to clarify that we use the word *measure* here as a synonym to *control*. To be precise, there is a difference, which we will discuss in the context of the changes that we made to the concept map in the next chapter (5.6). The measures were analyzed in detail in chapter 6. Therefore, diagram 5.5 only gives a small overview of the three categories (Technology, Process, and People) among some examples.

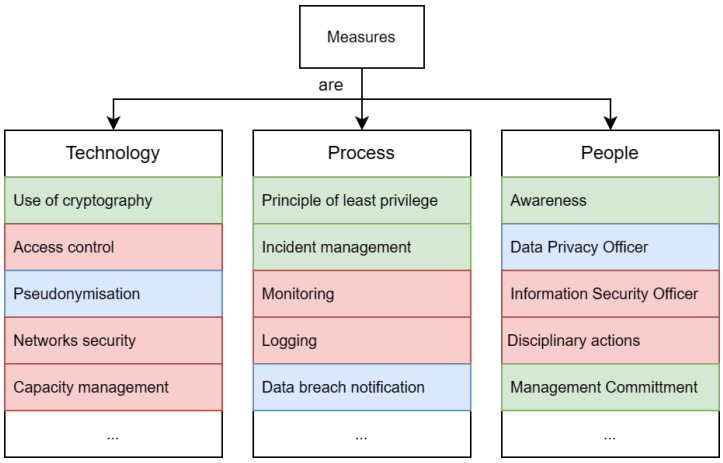

Figure 5.5.: Snapshot of the *measures* dimension in the concept map.

This list is non-extensive, and we refer to the different frameworks which describe measures in more detail.

[27] There are also some further frameworks belonging to the NIST Special Publication 800-series. An overview of other cybersecurity and privacy frameworks from NIST can be found here: `https://csrc.nist.gov/projects/cprt/catalog`

5.6. Versions of Concept Map

As already mentioned, there were multiple versions of the concept map. For improved visibility, we decided not to include the details of each dimension in the *general view*. Those are contained in each *detailed view* that was presented in the corresponding section above. Figure 5.6 shows the initial general overview of the concept map.

The feedback workshop provided some valuable insights, which led to the further differentiation between legal and customer requirements. The changes are highlighted in red in figure 5.7. In the same context, we added one important framework that is mainly used in the U.S. This can be seen in the detailed view of the *Requirements* and *Frameworks* dimensions in figure 5.8.

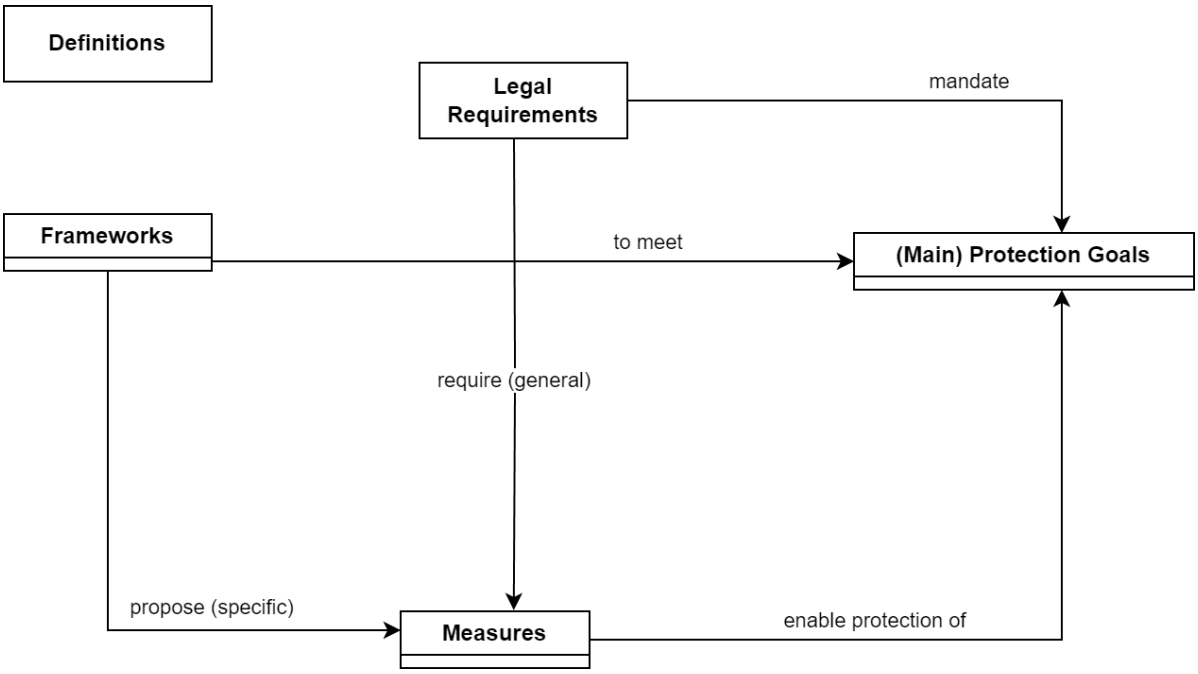

Figure 5.6.: General view of the initial version of the concept map.

The next improvements were achieved with the help of expert interviews. I-5 proposed to add the GDPR principles to the concept map. After some consideration, we decided to include further privacy principles in the context of their corresponding frameworks. This extended the figure 5.8 to the final version, represented by figure 5.9.

One approach was to add *Risks* to the concept map. Therefore, we asked the interviewees where they would put this.

In the first interview with I-1, the comment was that we should consider differentiating between controls and measures. While frameworks typically refer to controls, those controls describe how measures should be implemented to reduce risks. Also, controls often contain ways to evaluate the effectiveness of the measures. To put it in another way, the measure itself can be seen as the implementation of the control. We further developed this approach

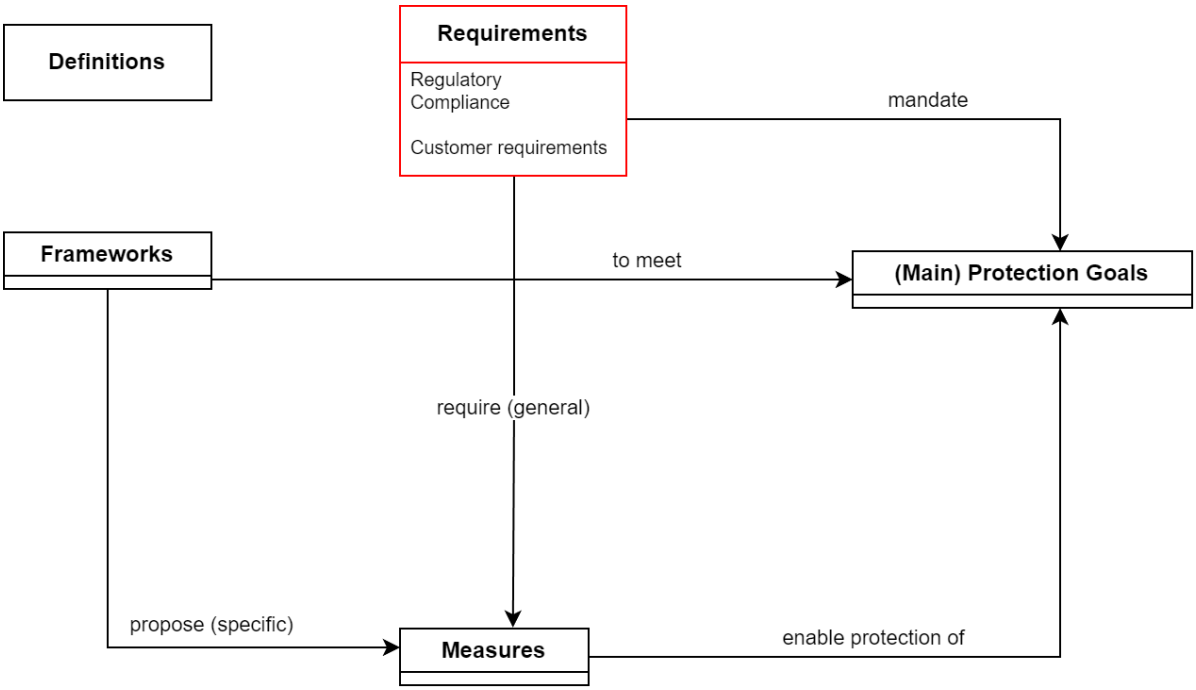

Figure 5.7.: General view of the concept map with additions from the feedback workshop.

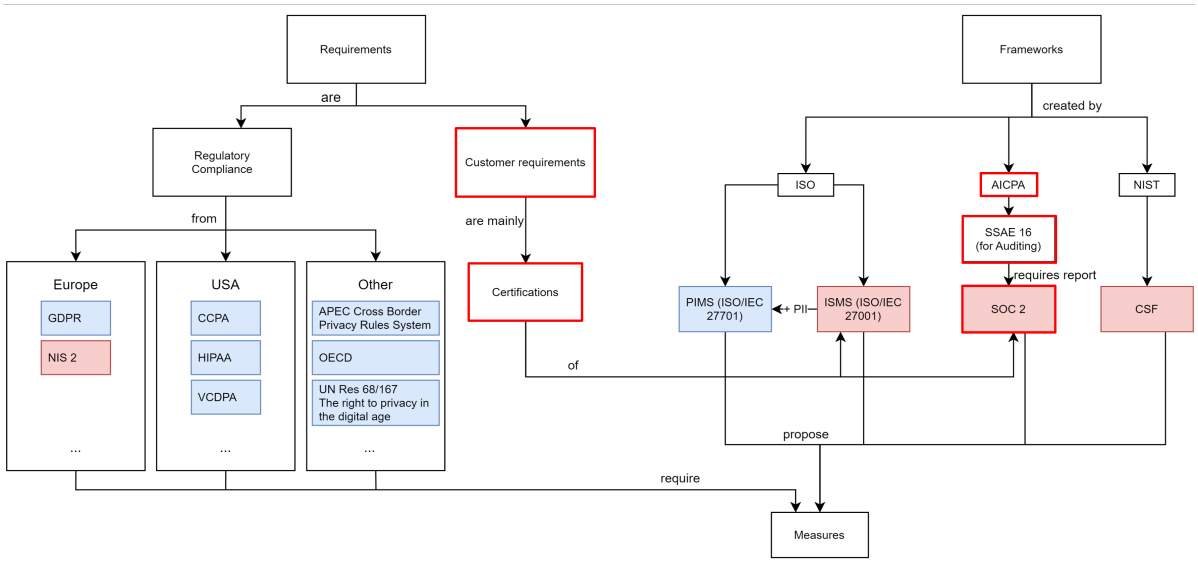

Figure 5.8.: Detailed view of the *Requirements* and *Frameworks* dimensions of the concept map with additions from the feedback workshop.

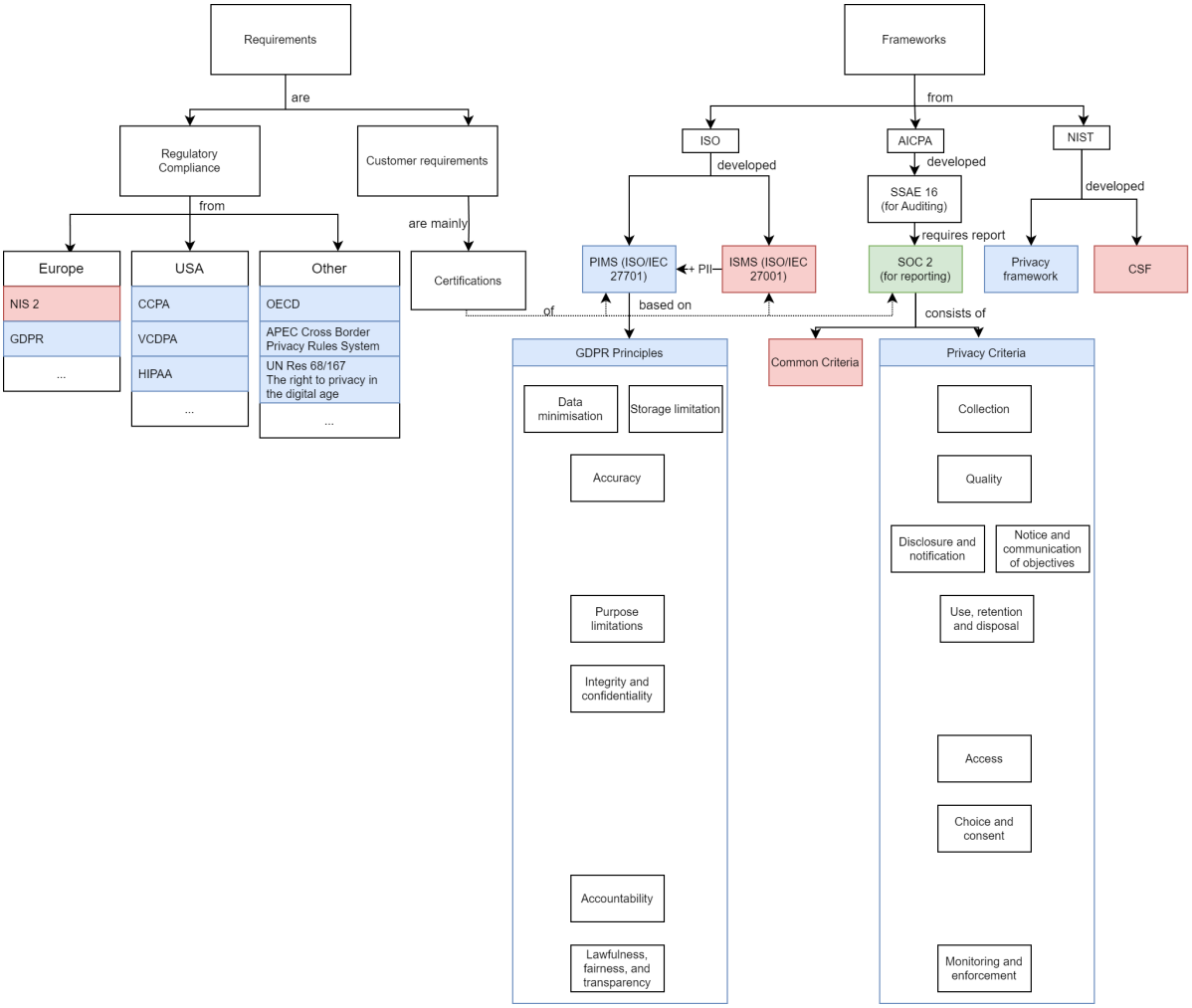

Figure 5.9.: Detailed view of the *Requirements* and *Frameworks* dimensions of the concept map with additions from the interviews.

to be represented in the concept map to also include the business context by adding the *control scope*. This is necessary because it is impossible to cover all possible threats in practice. Instead, a risk-based approach is needed, where prioritization is done and a scope is defined. Risks that fall out of this scope are called *accepted risks*. [28] In the interview with I-3, we further modified this approach and decided to keep *Controls / Measures* as the heading. The result can be seen in figure 5.10.

The other interviewees agreed with this approach to represent *Risks* next to *Controls / Measures*. I-6 had a different approach: He mentioned that risks are more connected to the *Requirements* because a "requirement may arise from a risk, which in turn leads to a measure that serves to achieve the protection goals." This introduced a risk-requirement-control/measure cycle, which is like the process of risk management. This was then again confirmed during the second part of the interview with I-1, who liked this inclusion, as it is analog to the "Plan Do Act-Cycle". By combining both suggestions, we reached our final version of the general concept map that is represented in figure 5.11.

5.7. General concept map

With the different versions of the concept map explained, as well as the different aspects in detail, this section gives a short description of the relationships. Because the *Definitions* influence every aspect of security and privacy, we did not visualize any relationship in the concept map.

Other than that, everything revolves around the *(Main) Protection Goals*. The *Requirements* mandate them, on the one side from a legal standpoint, but also from a customer and risk-based perspective. These *Requirements* often require the implementation of *Controls / Measures*, but they keep a rather general approach by maintaining technology neutrality. More specific controls are proposed in the different *Frameworks* [29], which have the same intention to meet the *(Main) Protection Goals*. The *Controls / Measures* are then implemented and applied based on the *Scope*, which is determined by the different *Risks*. With these *Controls / Measures*, we try to achieve the *(Main) Protection Goals*. As described previously, we also have a representation of the risk management process in the *Risks - Requirements - Controls / Measures* cycle.

A quote from I-2 shortly summarizes this: "[P]rotection goals are mandated from requirements. [...]. Then there are [...] frameworks[...] and then there are measures that come from those frameworks that enable that protection."

[28] To make this more tangible: Because of the different protection needs of assets, some can be left out of scope. One example of this would be a canteen plan, which is intended to be accessible by company-intern members. Still, there does not need to be further protection, as a leak of it would not cause any damage. Other information that is on the same company-intern classification level might need further protection, e.g., an internal employee distribution list that contains the email addresses of all employees.

[29] There are also indirect connections between the protection goals and the frameworks, as the *"privacy-specific" aspects* are very vague and therefore often relate to *privacy principles*, which are introduced in the privacy *Frameworks*.

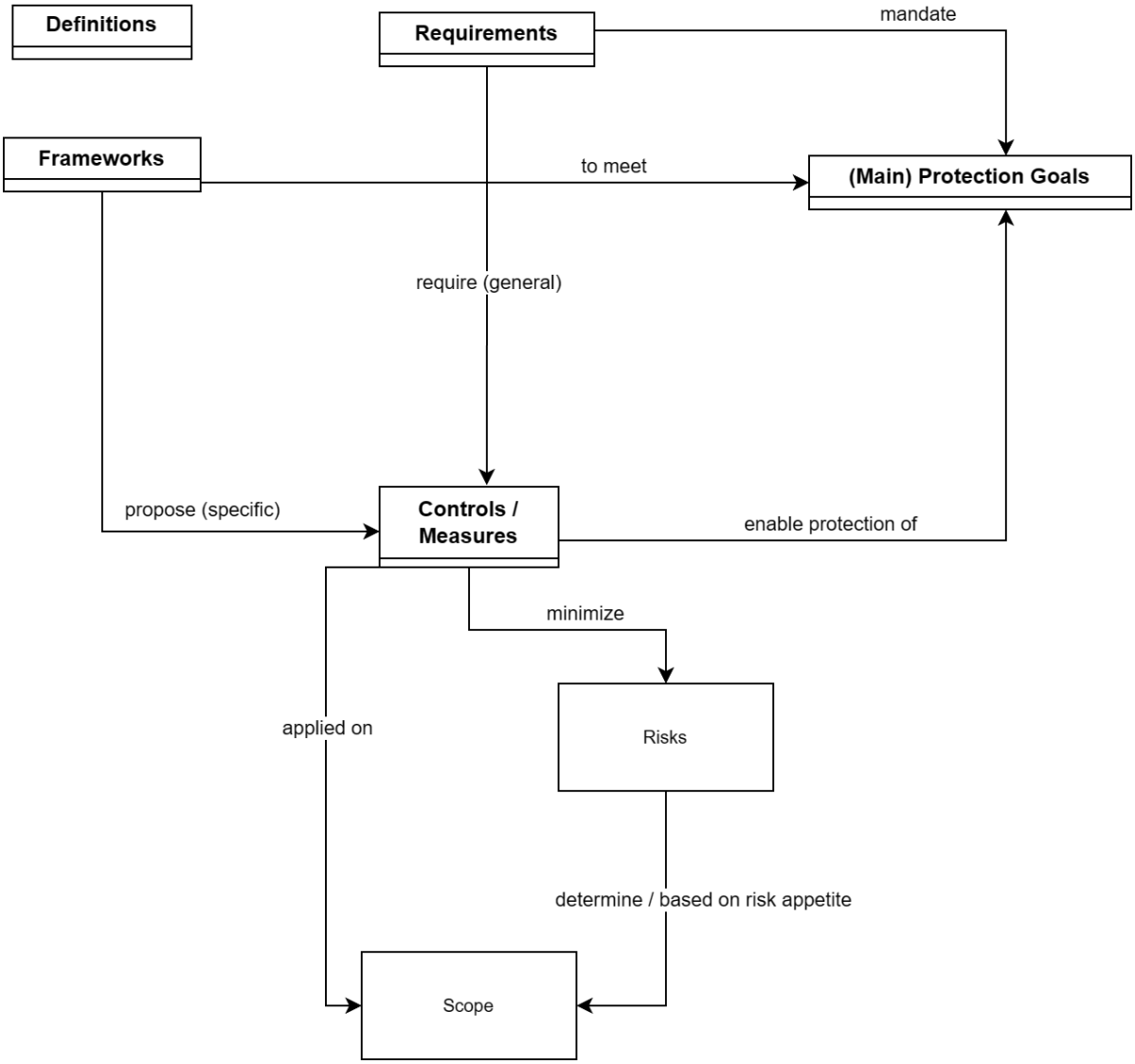

Figure 5.10.: General view of the concept map with the first additions from the interviews.

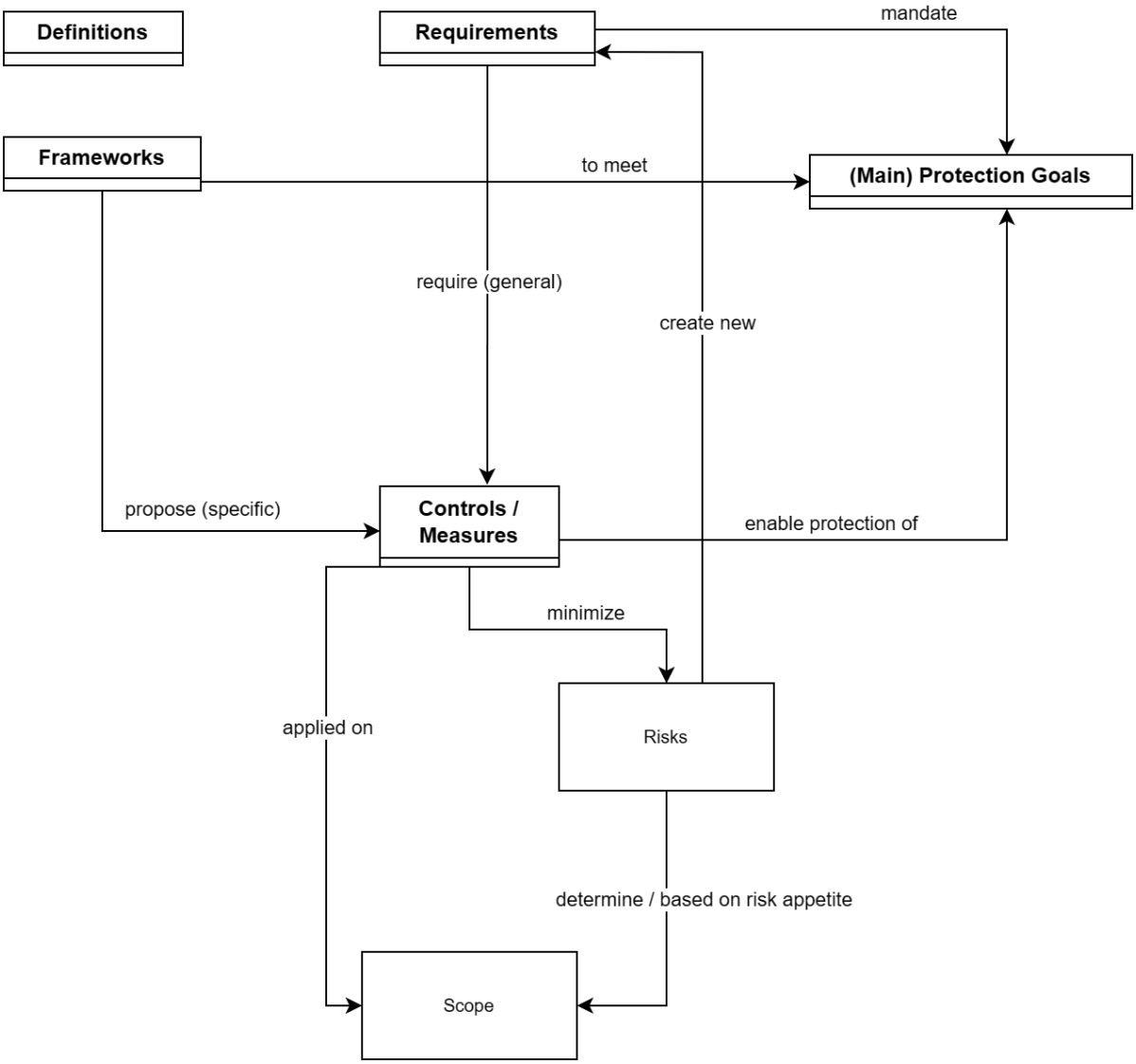

Figure 5.11.: Final version of the general view of the concept map.

6. Evaluation of ISO 27001 Controls

6.1. Evaluation Method

As already announced in the methodology chapter, the idea was to create a decision tree to have a uniform process to analyze the possible impact that ISO 27001 controls have on privacy. For that, we arranged a further discussion with security expert I-1 to find out how privacy topics are handled in the context of an ISMS.

This revealed that the metric that decides if further privacy impact needs to be evaluated (e.g., by performing a Privacy Impact Assessment) is the involvement of PII. Most privacy discussions are triggered, therefore, during the initialization phase of projects. This is relevant to the information security department, as the special protection of PII is also part of the ISO 27001 controls [1] and the involvement of PII automatically leads to a high confidentiality rating.

In the cooperation that I-1 works for, those privacy topics are currently mainly handled from a compliance standpoint. Therefore, their information security department often collaborates with the compliance department when privacy issues arise. In these deeper evaluations, the primary goal is to find solutions to stay GDPR compliant so as to fulfill legal requirements.

The second aspect was already mentioned: due to the nature of PII, their involvement leads to a high confidentiality rating of the asset, from which the privacy issue arose. This again confirms the overlap between security and privacy when it comes to confidentiality.

The third insight that we got was that some conflicts cannot be solved. In these cases, there needs to be a risk-based compromise between security and privacy.

These results are visualized in figure 6.1.

This small decision tree was then modified and extended to be used as an analysis tool for the evaluation of ISO 27001 controls. The result is a three-layer decision tree (6.2) that is described in the following.

The first level is analogous to our findings about the current evaluation. Here, we ask if PII is being processed or stored. If that is not the case, we are concluding that the control has *likely no impact* on privacy. If PII is involved, we need to find out if the overlap results in conflicts or synergies.

[1] In the 2013 version of ISO/IEC 27001, PII was addressed in chapter 18.1.4. The newer version from 2022 not only covers this in 5.34 but also introduces privacy considerations as part of the guidance in various other controls. In this frame, we also want to stress again that privacy topics are increasingly part of the new versions. This is also reflected in the changed overarching name of the latest update of the ISO/IEC 2700X standards: "Information security, cybersecurity and privacy protection".

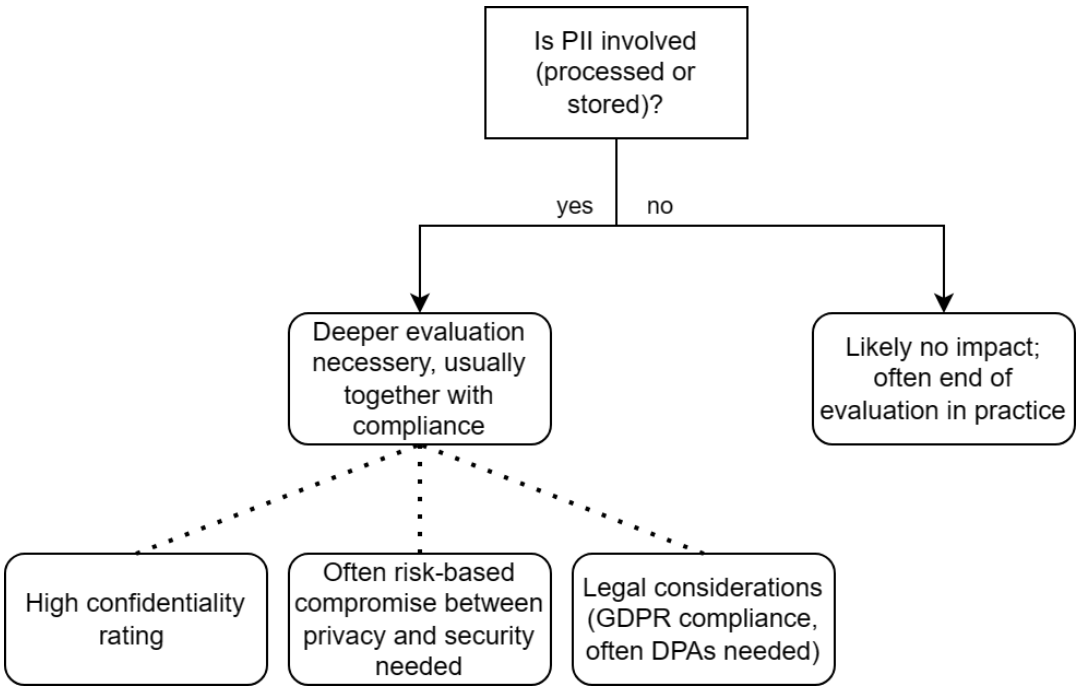

Figure 6.1.: Evaluation of privacy considerations in companies.

For the second step, we ask if any privacy aspect is negatively affected. To be able to answer this, we included the privacy aspects, consisting of the six privacy principles directly deriving from the privacy definition (Right to be let alone, Limited Access to the Self, Secrecy, Control Over Personal Information, Personhood, and Intimacy) and the most prominent privacy principles (Data minimization, Lawfulness, Fairness and Transparency, Purpose limitations, Accuracy, Storage limitation, and Accountability). We also added a list of supporting questions regarding the seven privacy principles on the left to further help with the decision in this second layer.

If no privacy principle is breached, we conclude that there is an overlap that does not result in conflicts. Here, the next evaluation is to differentiate if there are already **synergies**, if privacy is already directly considered in the security control, or if they could be added (*possible synergies*).

In case the answer to level two is *yes*, there is a *possible conflict*. The question that results in most possible conflicts was "Is further PII created?"

The third decision is to determine if this *possible conflict* can be solved. This is done in most cases by applying privacy methods, e.g., by encrypting the newly created PII. In cases where we can indeed restore privacy, we call this a *possible use case for PETs*, as this technology enhances privacy. If we cannot resolve this conflict, there needs to be a risk-based compromise between security and privacy. This evaluation is also part of the PET evaluation of chapter 7.

The final evaluation is to further differentiate if the identified **overlap** are already considered in the security control (**synergies**) or if they could be added (*possible synergies*).

As organizational controls only indirectly influence privacy while not involving PII, only following the decision tree for those controls would not identify their privacy impact. Therefore, we did a deeper investigation into these controls, which usually reference other controls that more directly affect privacy. This is not represented in the decision tree but reasoned in the corresponding control within the results section (6.3).

Another idea to improve this process resulted from the discussion with I-6 about the separation between PII and Sensitive Personal Information (SPI). Because not all kinds of PII need to be protected the same way, we included this in our considerations for the ISO control analysis. While no security mechanism creates SPI, we still wanted to highlight that there is a big range within the PII definition.

We differed on one side between the data of customers and the data of employees. For each, we then had a separation into three categories, listed by increasing sensitivity. Starting with the least critical, we differed between what we called “indirect PII”, meaning metadata like IP addresses. Then, we have an own category, which contains collected names. The remaining PII was called “direct PII”, including the traditional understanding of customer data like addresses or SPI.

While this differentiation did not influence the results of the evaluation, it was often a good indicator.

The final process is visualized in figure 6.2.

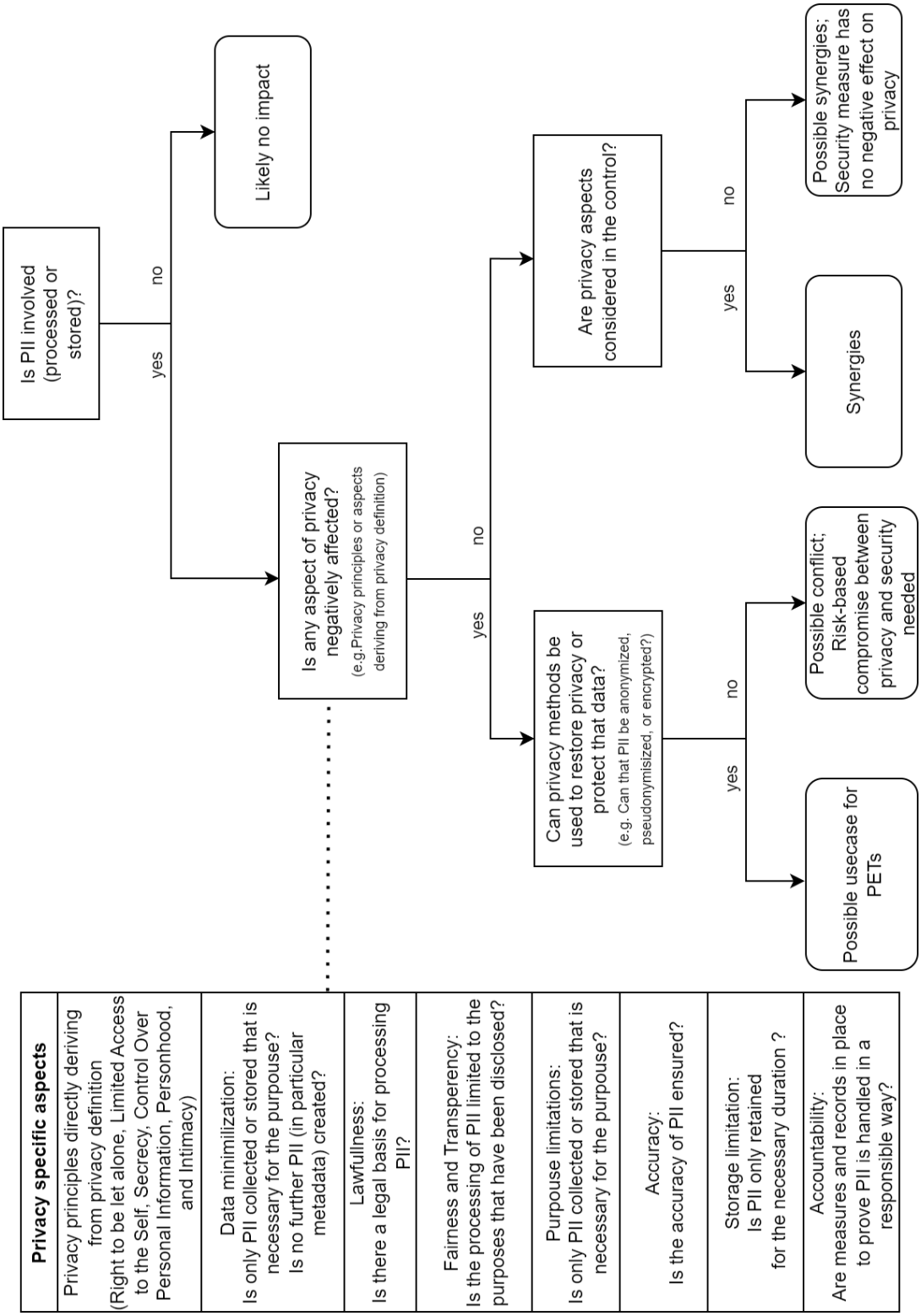

Figure 6.2.: Decision tree used to evaluate possible privacy impact of ISO 27001 controls.

6.2. Intended Use of the Results

Before discussing the results of our analysis, we want to highlight again that the identified possible conflicts neither intend to negatively portray the ISO/IEC 27001 or ISO/IEC 27002 frameworks nor to undermine their credibility. ISO provides the ISO/IEC 27701 that extends the ISMS to a PIMS, which includes additional measures and has the focus on privacy to create a GDPR compliant system.

Also, the identified conflicts themselves pose no violations of privacy laws, such as the GDPR. The latter specifically states that the processing of personal data with the goal to ensure information security "constitutes a legitimate interest"(Article 49 of [10]).

The analysis should instead support information security professionals that are implementing or maintaining an Information Security Management System and have an interest in maximizing privacy by highlighting specific aspects that need special privacy considerations during implementation, as the control may negatively impact privacy otherwise. This should also help to increase the awareness of privacy topics in areas where security is the priority. The analysis may often be very strict and suggest possible conflicts in areas where only a selected group of trustworthy employees have access that would not intentionally invade privacy. We still include those aspects because of the threats to privacy that this data might pose if the access is breached. [2]

The data created by security measures is meant to be only used when security needs it, e.g., during the analysis of security events. However, the concern is "that in theory, the data could also be accessed also without an incident." [I-1]

Another reason for this analysis is that is lays the basis for the following chapter 7.

6.3. Results of the Analysis

The results of the analysis are summarized in table A.3.

In the following, we briefly discuss each control where we identified a possible privacy principle breach and whether this conflict can be solved or not. As confidentiality is a protection goal for both security and privacy, as described in chapter 5.2, this analysis does not include this synergy unless the control specifically includes PII.

Segregation of duties (5.3)

This control proposes to segregate the duties and areas of responsibility within an organization. Thereby, it creates the foundations for role-based access and least privilege principles, which are introduced in (Control 5.15). [9] This control is an example of the previously mentioned organizational controls and only indirectly influences privacy.

[2] This argument is continued during the analysis of control about awareness (6.3) in section 6.3.

Contact with authorities (5.5)

This control requires to "establish and maintain contact with relevant authorities", mainly to report "identified information security incidents". [9] [3] As §33 of the GDPR also demands the "[n]otification of a personal data breach to the supervisory authority", [10] reporting processes, flows, and structures could be synchronized.

Contact with special interest groups (5.6)

This control is analog to 5.5 with the difference that the regulated contact is with "special interest groups". One example would be users whose data was leaked.

Information security in project management (5.8)

This control demands that "information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle". [9] This can be extended to the topic of privacy by integrating security and privacy considerations in those risk assessments.

Inventory of information and other associated assets (5.9)

This control describes that "[a]n inventory of information and other associated assets, including owners, should be developed and maintained." [9] This includes collecting names of information- and asset owners and thereby infringes the principle of *data minimization*.

Acceptable use of information and other associated assets (5.10)

This control "ensure[2] information and other associated assets are appropriately protected, used, and handled." [9] Therefore, all kinds of data are affected, as they should be handled according to the privacy principle of *purpose limitation*. Furthermore, the privacy principle of *accountability* is included, as this control includes that "should be responsible for their use" [9]

Return of assets (5.11)

This control requires "all the organization's assets in their [personnel] possession upon change or termination of their employment, contract, or agreement" to be returned. [9] In order to ensure this, there are two ways that privacy principles are breached:
1. Analog to 5.9, an inventory list is created, which contains the names of personnel who have company assets.
2. As it needs to be "ensure[d] that all relevant information is traced" [9], this could include a tracking of the company's devices, e.g., via GPS. This could be a privacy violation, as it might also track employees and therefore violate data *minimization principles*.

[3] To stress again: While the law often does not require security incidents to be reported (e.g., Loss of availability of internal printers), privacy incidents are. Security incidents that involve the loss of PII are also privacy incidents and need to be reported within 72 hours, according to the GDPR. [10]

Classification of information (5.12)

This control introduces information classification *"on confidentiality, integrity, availability"*. [9] This could be extended to a fourth category that is privacy-related, e.g., *containing PII"*.

Labelling of information (5.13)

This control describes the implementation of control 5.12. It can be argued that there are synergies with privacy, dependent on the definition of personal data. As discussed in chapter 5.1.2, intellectual property can belong to this category. If so, then this can be protected by the use of labeling, e.g., in the form of watermarks or via headers and footers. [9]

Information transfer (5.14)

This control aims to "maintain the security of information transferred". This control includes synergies, such as PII that are protected by the help of "cryptographic techniques (see 8.24)" or the special "consideration of any [...] relevant legal, statutory, regulatory and contractual requirements (see 5.31, 5.32, 5.33, 5.34)", such as Data Processing Agreements (DPAs). [9] But this control also violates *data minimization* by suggesting the "identification of appropriate contacts related to the transfer, including information owners, risk owners, security officers, and information custodians" [9]

Access control (5.15)

This control proposes "control physical and logical access to information and other associated assets" to "prevent unauthorized access" [9] By considering "which entities require which type of access to the information and other associated assets" (need-to-know / need-to-use principle) and only granting access to those necessary (least-privilege principles), important security measures are introduced. These principles also raise privacy, as they limit access to only the necessary people and systems. This can be seen as a form of assuring *purpose limitation* and *data minimization*. Also, the aspects of *secrecy* are a priority for this and the next three controls, which regulate the access to information (5.16, 5.17, and 5.18). But this control references the use of another one, in which security and privacy have conflicting requirements: Logging (8.15) violates the principle of *data minimization*.

Identity management (5.16)

This control describes the management of identities. While "identities assigned to persons [are] [...] only linked to a single person" [9] at a time, this is also reflected in the privacy principle of *accountability*. Also, the principle of transparency is met by keeping "records of all significant events concerning the use and management of user identities and authentication information". [9] While this does not directly represent the *transparency* principle, it supports it by guaranteeing that digital identities also represent the correct corresponding natural identity. On the other hand, this control works on names, which should be protected.

Authentication information (5.17)

This control is about the "[a]llocation and management of authentication information". [9] While the guidance also includes the importance of strong passwords and password management systems, the possible privacy violation is in the *other information*: It suggests the use of "biometric data such as iris scans or fingerprints." [9] This itself is no problem, but if this authentication mechanism is enforced as being mandatory by an organization, this would conflict with the conception of privacy deriving from the *Limited Access to the Self* in chapter 5.1.2.

Access rights (5.18)

This control handles the "provision[ing], review, modifi[cation] and remov[al]" of access rights. [9] It mainly focuses on the theoretical distribution of access rights By "maintaining a central record of access rights granted to a user identifier (ID, logical or physical) to access information and other associated assets" as well as "maintaining a record of changes to users' logical and physical access rights", the *transparency* principle is addressed.

Information security in supplier relationships (5.19)

This control ensures that "an agreed level of information security in supplier relationships" is maintained. [9] Therefore, "information security risks associated with the use of supplier's products or services" are managed. This could be easily extended to privacy topics, which is why we see possible synergies here.

Addressing information security within supplier agreements (5.20)

This control is similar to 5.19 but focuses on the information security within the suppliers by proposing to include "information security within supplier agreements". [9] Analog to 5.19, there are synergies, which are already utilized because this control already includes "data protection" requirements and specifically mentions the "handling of personally identifiable information (PII), intellectual property rights and copyright". One example of that is DPAs, which could be considered in this context.

Managing information security in the ICT supply chain (5.21)

This control applies 5.19 to the whole ICT supply chain. [9] Therefore, it includes the same potential synergies that could benefit privacy by considering not only security requirements.

Information security for use of cloud services (5.23)

This control sets specific considerations for using cloud services. [9] There are synergies, as the "PII protection in public clouds" should also be considered.

Information security incident management planning and preparation (5.24)

This control describes the planning and setting up of structures to "manag[e] information security incidents". [9] Some of the preparations involve references to other controls, where conflicts between information security and privacy are, in particular, "monitoring (see 8.15 and 8.16), detecting (see 8.16), [...] reporting (see 6.8)", and "handling of evidence (see 5.28)". "[R]oot cause analysis or post-mortem" procedures are also mentioned, which are also conflicting to *data minimization*. On the other side, *transparency* is guaranteed by "logging incident management activities".

Response to information security incidents (5.26)

This control introduces the steps performed for an "efficient and effective response to information security incidents." [9] While there are again synergies with the *transparency* principle due to the logging of incident response activities, there is again another control mentioned, where conflicts arise regarding the collection of evidence (5.28).

Collection of evidence (5.28)

This control gives guidance on establishing and implementing "procedures for the identification, collection, acquisition, and preservation of evidence related to information security events." [9] There are several steps that - while being necessary - can violate privacy principles. The *data minimization* principle is violated during the "identification, collection, acquisition and preservation of evidence", because this involves a deeper analysis of not only logged metadata but sometimes also the users' data itself (e.g., a downloaded file, which contains any malware). Also, this data is sometimes stored for a longer time if this digital evidence is necessary in any legal cases - if this data contains PII, it must not be deleted, which theoretically conflicts with the privacy aspects for *data retention*.

Legal, statutory, regulatory and contractual requirements (5.31)

This control "ensure[s] compliance with legal, statutory, regulatory and contractual requirements related to information security" [9] By extending the control to also privacy requirements, synergies could be utilized by having combined processes. But there is one big possible conflict when it comes to cryptography, which is mentioned in its own section of this control. Special consideration of "mandatory or discretionary methods of access by the countries' authorities to encrypted information" is advised. [4] This means that while both

[4]Some countries have stricter encryption laws than others. In Germany "telecommunications service providers must be able to decode any telecommunications which are protected through technical measures", but personal data is still protected by the GDPR. In the US, there is no such rule, but because the "interception of communications and delivering intercepted communications to the government" is a legal requirement, governmental agencies then are allowed to encrypt this data anyways. [53]

security and privacy benefit from cryptography, the privacy component is partly revised again through this control. [5]

Intellectual property rights (5.32)

This control "protect[s] intellectual property rights." [9] The *secrecy* overlaps with privacy, which would be positive, depending on whether the definition of personal data includes intellectual property.

Protection of records (5.33)

This control handles the protection of records "from loss, destruction, falsification, unauthorized access, and unauthorized release." [9] Therefore, not the control itself, but rather the obligation that it implements can conflict with privacy. Because the *records* can also include PII, special consideration needs to be given to maintain privacy, particularly considering the right to access, correction, or data retention. On the other side, this control tries to minimize the added possible privacy complications by including a "retention schedule" and promoting the protection of the records by encryption (8.24).

Privacy and protection of PII (5.34)

This control mandates to "identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements." [9] This is mainly motivated by the compliance to "relevant legislation and regulations concerning the preservation of privacy and protection of PI". [9] Regardless, as this control demands PII protection, there are clear synergies to privacy, especially for *secrecy*. The control also recommends the appointment of a "privacy officer", which is often a privacy requirement. While this control calls it "[r]esponsibility for handling PII", this represents the *accountability* privacy principle.

Screening (6.1)

This control "ensure[s] all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment." [9] It involves background verification checks, as well as intensive screening procedures. While this control already regulates itself by taking into "consideration all relevant privacy, PII protection and employment-based legislation" requirements, it still involves the collection of personal data, which is against the principle of *data minimization*. Also, the conception of *personhood* might be invaded if the screening is done to a disproportionately large extent, in particular, if any prejudices influence the outcome of this process.

[5] We would argue that the security component is kept in most cases because, usually, governments do not attack companies and, therefore, are not seen as threats. Privacy, on the other hand, also relates to the data of individuals, and - in addition to the attack vectors information security has - governments can breach that. This was also mentioned by I-5 during the interviews.

Terms and conditions of employment (6.2)

This control, which helps "personnel [to] understand their information security responsibilities" [9], can be extended to privacy principles, which makes this an area with possible synergies.

Information security awareness, education and training (6.3)

This control handles the "security awareness, education and training" [9]. Starting with some synergies, training could also "be part of, or conducted in collaboration with, other activities, for example, general information management, ICT, security, privacy, or safety training.". One possible privacy conflict arises if the usernames in the learning management system (LMS) often contain personal data. That results in being able to see who did and who did not finish the training. While this application may not pose a too big risk, other than giving attackers a list of potentially weaker, it would not be difficult to apply *data minimization* and avoid the collection of PII e.g., by masking the usernames with IDs. Another example where this is even more critical is in the context of awareness phishing simulations. [6]

Disciplinary process (6.4)

This control allows to "take actions against personnel and other relevant interested parties who have committed an information security policy violation." [9] At first look, this might be problematic for the privacy of perpetrators, but the control solves the biggest part of this problem by further adding that "[w]here possible, the identity of individuals subject to disciplinary action should be protected in line with applicable requirements." Still, the names of perpetrators are needed, in particular in cases of unintentional breaches, to assign further awareness measures to them.

Confidentiality or non-disclosure agreements (6.6)

This control protects information by introducing "[c]onfidentiality or non-disclosure agreements." [9] As the information protected by that can also consist of PII, or - depending on the definition - intellectual property, there are synergies to the privacy principle of *secrecy*.

Remote working (6.7)

This control describes in detail considerations to "ensure the security of information when personnel are working remotely." [9] The high focus on confidentiality leads to synergies with the privacy principle of *secrecy*.

[6] In those simulations, the security department sends (harmless) phishing emails to employees. The emails usually contain a link to a website with a login form. If not configured correctly, the names of employees who clicked are recorded, including their entered passwords. While it may be helpful to receive the names of people who clicked and fell for the phishing simulation to provide them with further training, many tools can already do this automatically. Because they do not need further human involvement, this allows the users' data to be masked and further protected.

Physical entry (7.2)

This control handles the physical entry to secure areas, which "should be protected by appropriate entry controls and access points." [9] There are conflicts to privacy by "maintaining and monitoring a physical logbook or electronic audit trail of all access." By tracking *who* accessed *when*, further assumptions could be made, e.g., regarding the work performance of employees. This is against the *data minimization* principle and would be a big invasion of privacy. Another area of conflict with the *Limited Access to the Self* conception could occur if biometric authentication mechanisms were demeaned. Furthermore, "inspecting and examining personal belongings of personnel and interested parties upon entry and exit" could also invade privacy in some cases.

Physical security monitoring (7.4)

This control uses "surveillance systems" to "detect and deter unauthorized physical access." [9] This violates the *data minimization* principle, but for its implementation "local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods" should also be considered.

Clear desk and clear screen (7.7)

This control gives guidance on how "[c]lear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced" [9] This reduces the exposure of information, including PII, to a minimum of people and therefore has synergies to the *secrecy* conception.

Security of assets off-premises (7.9)

This control aims to increase the protection of "[o]ff-site assets". [9] Analog to 5.11, "location tracking [...] of devices" should be considered. Collecting location data of devices is against the principle of *data minimization*. Also, "maintaining a log that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment" violate that aspect.

Storage media (7.10)

This control is about the protection of "information on storage media." [9] Synergies are in the *secrecy* context; "cryptographic techniques" are promoted. There is also some advice for ensuring a "[s]ecure reuse or disposal".

Secure disposal or re-use of equipment (7.14)

This control extends the methods for secure disposal or re-use, that 7.10 introduced. "In addition to secure disk deletion, full-disk encryption reduces the risk of disclosure of confidential

information when equipment is disposed of or redeployed". [9] That leads to synergies with the *secrecy* principles as the protection of PII increases.

User endpoint devices (8.1)

This control gives details on the protection of user endpoint devices. One privacy conflict is the consideration of "end user behaviour analytics (see 8.16)". [9] This contradicts the *data minimization* principle. But this control also suggests the "use [of] privacy screen filters". In the context of the usage of personal devices (BYOD), "PII protection legislation should be considered".

Privileged access rights (8.2)

This control helps in restricting and managing the "allocation and use of privileged access rights". [9] In that frame, we see two conflicts with *data minimization*: Not only is a "record of all privileges allocated" maintained, which includes names, but also a "logging [of] all privileged access to systems for audit purposes" performed.

Information access restriction (8.3)

This control restricts the access to information. For sensitive information, "anonymous access" is forbidden, which enhances *accountability*, but in turn, of course also conflicts with privacy. Another possible conflict is "monitor[ing] the use of [...] information", which is extended to a "recording who accesses the information and how the information is used". [9] This is against *data minimization*.

Access to source code (8.4)

This control manages "[r]ead and write access to source code". [9] Thereby again, the *data minimization* principle is jeopardized by maintaining "audit log of all accesses and of all changes to source code". On the other side, this leads to an increased *accountability*.

Secure authentication (8.5)

This control "ensure[s] a user or an entity is securely authenticated, when access to systems, applications and services is granted." [9] The effect on *data minimization* and *accountability* are like in the previous controls, due to "logging unsuccessful and successful attempts" of authentication. Furthermore, the use of biometric methods is suggested, which could conflict with *Limited Access to the Self* if made necessary.

Capacity management (8.6)

This control describes how the "use of resources should be monitored and adjusted in line with current and expected capacity requirements." [9] Because "monitoring should be applied

to ensure and, where necessary, improve the availability and efficiency of systems", this could contradict the *data minimization* principle.

Protection against malware (8.7)

This control handles the "[p]rotection against malware [...] supported by appropriate user awareness." [9] As this involves "implementing controls that prevent or detect the use of known or suspected malicious websites (e.g., blocklisting)", "scanning any data received over networks", "scanning email and instant messaging attachments and downloads", "scanning webpages [...] when accessed", the principle of "data minimization" is violated. Often, for this control, the whole incoming and outgoing internet traffic is analyzed.

Information deletion (8.10)

This control explains the process of information deletion. By this, it "prevent[s] unnecessary exposure of sensitive information and [...] comply[s] with legal, statutory, regulatory and contractual requirements for information deletion." [9] That way, synergies with *data retention* and *secrecy* exist. It further refers to "ISO/IEC 27555" for additional guidance on the deletion of PII.

Data masking (8.11)

This control introduces the methods to "limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements." [9] The whole control could have originated from a privacy framework, as it describes privacy "techniques such as data masking, pseudonymization or anonymization" to protect sensitive data like PII. Also, other methods to protect data include, e.g. encryption, substitution, hashing, or data obfuscation. Summarized, there are synergies with *secrecy*.

Data leakage prevention (8.12)

This control gives guidance on how to apply data leakage prevention measures to "detect and prevent the unauthorized disclosure and extraction of information by individuals or systems." [9] Encryption is also recommended during backing up data to protect sensitive information, like PII. Due to the focus on PII protection, synergies to *secrecy* exist.

Information backup (8.13)

This control proposes the backup of information. While mainly focusing on availability and preventing the "loss of data and systems", there might arise conflicts when data that is part of backups needs to be deleted. The control itself considers parts of this: "The retention period for essential business information should be determined, taking into account any requirement for retention of archive copies. The organization should consider the deletion of information (see 8.10) in storage media used for backup once the information's retention period expires

and should take into consideration legislation and regulations." [9] While this addresses some of the mentioned problems, it leaves the conflict that the right to erasure might not be technically enforced on data that is part of backups. *Data retention* of Personal Identifying Information is therefore in conflict.

Logging (8.15)

This control was already mentioned several times earlier. It promotes the use of "[l]ogs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analy[z]ed." [9] There are conflicts with *data minimization* because logging creates and stores metadata, including PII. The control further tries to protect these logs with "cryptographic hashing, recording in an append-only and read-only file, recording in a public transparency file". Also, log analysis is described, considering, e.g., "security information and event management (SIEM) or firewall rules, and intrusion detection systems (IDSs) or malware signatures", or "known behavi[o]r patterns and standard network traffic compared to anomalous activity and behavi[o]r [user and entity behavi[o]r analytics (UEBA)]". On the other hand, *accountability* is improved.

Monitoring activities (8.16)

This control describes how "[n]etworks, systems and applications should be monitored for anomalous behavi[o]r and appropriate actions taken to evaluate potential information security incidents." [9] This can jeopardize privacy, as not only metadata is analyzed but also documented with monitoring records, which contradicts *data minimization*. Monitoring and analysis themselves can be automated, and therefore, the level of privacy is dependent on its configuration.

Networks security (8.20)

This control handles network and security devices that "should be secured, managed and controlled to protect information in systems and applications." [9] By considering "appropriately logging and monitoring to enable recording and detection of actions that can affect, or are relevant to, information security (see 8.16 and 8.15)", the principle of *data minimization* is conflicted.

Security of network services (8.21)

This control introduces "[s]ecurity mechanisms, service levels and service requirements of network services". [9] As "monitoring of the use of network services", including "time, location and other attributes of the user at the time of the access" are metadata and PII, this contradicts the *data minimization* principle.

Web filtering (8.23)

This control also manages the "[a]ccess to external websites". [9] As the blocking of restricted websites is monitored and usually counts as a security event, this poses a further conflict to *data minimization*.

Use of cryptography (8.24)

This control "ensure[s] proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography." [9] This results in synergies with *secrecy* because PII is protected.

Application security requirements (8.26)

This control describes "[i]nformation security requirements [which] should be identified, specified and approved when developing or acquiring applications." [9] It further extends the requirements introduced during Information security in project management (5.8). By considering the "need for privacy associated with all parties involved", there are already synergies implemented.

Secure system architecture and engineering principles (8.27)

This control contains "[p]rinciples for engineering secure systems should be established, documented, maintained and applied to any information system development activities." [9] Some synergies are already contained "(e.g. [the] encryption of sensitive information" but could be extended by further privacy techniques (e.g., privacy by design, together with "security by design") to adding harmonize security and privacy.

Separation of development, test and production environments (8.31)

This control "protect[s] the production environment and data from compromise by development and test activities" by separating and securing "testing and production environments". [9] One aspect that is mentioned to achieve this prohibits "copying sensitive information into the development and testing system environments unless equivalent controls are provided for the development and testing systems". This protects PII and which has synergies with *secrecy*.

Test information (8.33)

This control demands that "[t]est information should be appropriately selected, protected and managed." [9] There are synergies to privacy by the rules protecting "[s]ensitive information (including personally identifiable information)", which was introduced in 8.31.

6.3.1. Summary of the results

- We could identify in total 30 possible conflicts:
  5.9, 5.11, 5.14, 5.15, 5.16, 5.17, 5.24, 5.26, 5.28, 5.31, 5.33, 6.1, 6.3, 6.4, 7.2, 7.4, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.13, 8.15, 8.16, 8.20, 8.21, and 8.23
- 36 synergies were found: [7]
  5.3, 5.5, 5.6, 5.10, 5.13, 5.14, 5.15, 5.16, 5.17, 5.18, 5.20, 5.23, 5.24, 5.26, 5.32, 5.33, 5.34, 6.6, 6.7, 7.7, 7.10, 7.14, 8.1, 8.2, 8.3, 8.4, 8.5, 8.10, 8.11, 8.12, 8.15, 8.24, 8.26, 8.27, 8.31, and 8.33
- 6 Areas were found where synergies are possible:
  5.8, 5.12, 5.19, 5.21, 5.31, and 6.2

[7] The first three controls had indirect synergies. If the main goal of the security measure was confidentiality, often an overlap occurred, e.g., with secrecy.

7. PET Assessment

The first part of this chapter is to find solutions to the identified possible conflicts of the previous chapter. We tried to investigate if and which privacy methods could solve these.

7.1. Treatment of possible conflicts

Control 8.11 describes the differences between anonymization and pseudonymization: "[a]nonymization irreversibly alters PII in such a way that the PII principal can no longer be identified directly or indirectly." [9] According to the GDPR, such data does not count as PII anymore if the identification is removed, thereby reducing its protection needs. This makes it a good fit for controls, where data is collected and analyzed for improving availability, e.g., to learn general user behavior or capacity management.

In 6 cases, anonymization would be possible:
7.4, 8.1, 8.3, 8.6, 8.15, and 8.23 [1]

When the data needs to be traced back to individuals in cases of identified breaches or to ensure transparency or accountability, pseudonymization is better suited. By "replac[ing] the identifying information with an alias", PII is protected, and only a link to the actual person is drawn when needed.

In 19 cases, pseudonymization could solve the conflicts:
5.9, 5.11, 5.15, 5.16, 5.24, 5.26, 5.28, 6.3, 7.2, 7.9, 8.2, 8.4, 8.5, 8.7, 8.15, 8.16, 8.20, 8.21, and 8.23. [2]

In three other cases, we propose other solutions to the conflicts.

- 5.11: If the tracking of assets was not permanent but only activated in cases when necessary, the return of assets still would be guaranteed while not violating privacy.
- 5.17: If biometric authentication stays optional, then there is no conflict.
- 6.1: The screening process could maybe be improved by separating the data collection and the data evaluation steps. That way, information that would violate the *personhood* perception of privacy could be excluded in the first step. Due to the separation, this would not influence any decision. [3] Another option was found in another section and is described there. (Section 7.4)

[1] For 8.15 and 8.23, the use of pseudonymization or anonymization depends on the context of how these controls are implemented. Therefore, we added them to both categories.

[2] For some of the controls, there are more various aspects to them. Also, sometimes, multiple approaches can solve the issues. Therefore, they are listed in all of those categories.

[3] While this would contradict the *data minimization* principle in the first place - thus this is in the partly solvable

7.2. Summary of the results

- 20 of the identified possible conflicts could be solved:
  5.9, 5.11, 5.15, 5.16, 5.17, 5.24, 7.2, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.15, 8.16, 8.20, 8.21, and 8.23
- 5 were identified as partly solvable:
  5.26, 5.28, 6.1, 6.3, and 7.4
- 5 were identified as not solvable:
  5.14, 5.31, 5.33, 6.4, and 8.13

In a further step, we wanted to investigate if any PET could further help to support security measures.

7.3. List of PETs

First, we need a small overview of some PETs.

Lin et al. described privacy by applying the three different steps of data collection and use to the topic of privacy. Those steps are "1) data collection; 2) data aggregation; and 3) data mining and analytics". [26]

By doing that, they also introduced different privacy-preserving mechanisms, all belonging to the data aggregation category:

- Anonymity-based privacy preservation:
  K-anonymity, L-diversity, T-closeness, etc. [26]
- Encryption-based privacy preservation:
  homomorphic encryption, commitment mechanism, secret sharing, zero-knowledge proof, etc. [26]
- Perturbation-based privacy preservation:
  data customization, data sharing, random noise injection, etc. [26]

While many of these approaches are interesting, some are very novel and thus not much researched yet. Therefore, we want to focus more on PETs that are in a further development stage and add further PETs before applying them to the *conflicts* derived from the analysis of the previous chapter.

First we collect an overview of some PETs, ranked by their prevalence according to Fantaye [22]:

category - we still propose this option as we think that *personhood* is higher valued in most cases. Furthermore, this would minimize any negative effects that could arise from the privacy violation and, therefore, improve this situation.

- Federated Learning,
- Differential Privacy,
- Homomorphic Encryption,
- Secure Multi-Party Computation (SMPC),
- Zero-Knowledge Proofs,
- Trusted execution environments,
- Privacy-Preserving Data Mining,
- Private Information Retrieval,
- L-Diversity,
- Pseudonymization, and
- T-Closeness.

This list can be extended with the following PET from the Information Commissioner's Offices PETs guidance [11].

- Synthetic data

The goal of this thesis is not to describe any PET in detail or analyze their potential to increase security. Instead, the question is asked if some of these could help to solve the identified possible conflicts from our ISO 27001 control evaluation. [4]

We also want to highlight again that this part of the thesis did not follow a formal approach and, therefore, could also be seen as an early section of the discussion chapter.

7.4. On the Relationship Between PETs and Security Measure

Use cases for PETs

For this step, we went through the list of PETs and tried to find use cases for them by comparing the gain they bring to the requirements of each ISO control. We discovered the following possible use cases:

[4] There are many interesting examples for such use cases. One example is SMPC, in particular its subcategory of private-set intersection (PSI), which can help to identify if a user's password has been disclosed and needs to be changed to restore security. [57] Thinking this technique even further, PSI protocols need to be well designed to detect and prevent malicious behavior, as there is also the potential to misuse this technique. Imagine a malicious party that abuses this application by sending random combinations of characters with the goal of identifying passwords contained in the secure database that PSI wants to protect.

- *Zero-Knowledge Proofs* could be used during the data collection process of Screening (6.1). (E.g., to verify academic qualifications like degrees, identity, credit review, or review of criminal records). Also, when it comes to (security) certifications in the context of supplier relationships (5.19), such proofs could be used.
- The idea of *Zero-Knowledge Proofs* could also be implemented in the context of authentication methods regulating access. While this would enhance data minimization and prevent personalized logging, this would jeopardize the principle of accountability. We think that there might be more use cases for this and suggest deeper investigations.
- *Trusted execution environments* is a principle that probably arose from security and applies the approaches of controls like the separation of development, test and production environment (8.31), segregation of networks (8.22), or even the separation of physical security parameters (7.1) to the physical level of computer chips.
- *Pseudonymization* was already addressed and had many use cases, in our opinion.
- *Synthetic data* could be useful to create Test information (8.33).

Can PETs replace security measures?

A similar question was part of the expert interviews, which is what this section is addressing.

As the goal of PETs is to increase privacy, we created a thought experiment: Imagine that a technology exists in which we can achieve complete privacy. [5] Does this technology still need security?

I-5 argued that there is no "complete data privacy at all – just as there is no complete security, as it can never be guaranteed that data cannot be reconstructed or de-anonymized" [5] His argument was that with the "progress of technology" every security or privacy mechanism could be broken earlier or later. The example while explaining this was about the evolution of "processors [...] [which] can nowadays perform brute-force attacks on what was unimaginable just a few years ago – and quantum computing will completely change the game as well."

I-6 noted that the transmission to the shop would still require some security, "For example, if I were to say the shop is running on HTTP instead of HTTPS, even though the data might not be stored, it would still be transmitted over the network without encryption. Someone could potentially intercept it through a man-in-the-middle attack." [I-6] He also mentioned that for legal reasons, things like a "invoice at the end", "accounting, maybe [...] tax returns, [...] a balance sheet" still are necessary. We "still need a certain minimum level of processing, and in fact, storage". "Maybe if you don't need a database to store things, you don't have to worry about whether the database is secure or not, but then again, you can choose approaches where you try to store and process as little as possible, and then focus on security for that specific area, or at least scale it down."

[5] For example, an online shop that does not need to store or process any personal data. In this hypothetical scenario, a yet unknown PET is used that can handle the necessary tasks like the payment process or the labeling and sending of the product to the customer, so this is out of scope, and no PII would be involved.

I-1 reasoned rather shortly: "Yes, of course, I would say [that security is still necessary.] [...]. Because we have not only confidentiality but also integrity and availability. And we also have confidential data that is separate from personal data." [I-1] This reasoning was similar to the one from I-2: "We could still break that system by running a DDoS attack. [...] That would not infringe privacy but would destroy that shop." [I-2]

We can also apply those answers to describe the relationship between PETs and security measures more precisely. The general consensus was that privacy alone cannot replace the need for security due to the other protection goals that security has.

When it comes to specific applications of PETs, it again depends on both the measure, and the PET:

- If the measure has *availability* aspects, a PET is unlikely to ensure that.
- In cases where *integrity* or *availability* is prioritized, we can see that certain PETs and privacy measures will be integrated to security. But instead of *replacing*, they are rather added as further protection on top. This is already the case, as the ISO control analysis showed. *Pseudonymization* was integrated as part of the *Data masking* control (8.11).

To summarize, we want to mention again that PETs are designed often for very specific use cases. If they happen to match the requirements of security controls, they could indeed replace them. But we think that a more likely scenario is that the security measure would change and adopt the PETs rather than being replaced by it. If that counts as "PETs replacing information security measures" is up to debate.

8. Discussion

This chapter contains two sections: First, we will discuss the key findings and their possible implications. Secondly, the limitations of this thesis are addressed.

8.1. Key findings

8.1.1. Confidentiality Overlap

We discussed that both, security and privacy, have the goal of protecting the confidentiality of data. While security involves all data, privacy calls this principle *secrecy* and only focuses on PII. In this aspect, privacy is a subcategory of security. Security experts also confirmed this theoretical relationship during the feedback workshop and the interviews. Even the results of the ISO measure analysis seem to support this further:

One finding was that many synergies arose when the confidentiality aspect of the security measure was the priority. Areas where conflicts were identified often valued other protection goals more. This again confirms the *confidentiality overlap*: The privacy principle of secrecy and the security protection goal of confidentiality go hand in hand.

8.1.2. Past and present evolution of requirements: Best practices

It appears that the stakeholders, who primarily set requirements for security and privacy, have changed over time.

Information security in companies mainly developed as a form of (IT) risk management, intending to find the right balance between spending money to protect against a security breach and the resulting potential monetary loss. Therefore, if the spending was lower than the expected loss, the company minimized its opportunity costs and implemented security measures. This developed from the inside of companies and became best practice.[1] In the same way, many of the recommendations for security measures came up. While there were also some guidelines published by governmental institutions, like NIST, their compliance was mainly voluntary.

With the "increasing importance of information and communication technology", in parallel with "new threats" [2], governments started being involved and setting up rules to protect governmental institutions. [45] These protection rules were then extended to critical infrastructures, e.g., by the German KRITIS. The upcoming NIS 2 again increases the scope of

[1] And this is still being carried on e.g., by the automotive industry. - See section 5.3.1

[2] The growing number of more organized cyberattacks, as well as the attack of whole countries IT infrastructures nation-coordinated cyber war demand governments to develop strategies for protection.

governmental requirements for information security, which suggests that this evolution will continue. One interesting observation is that these new legal requirements for information security mainly focus on availability. [3]

8.1.3. Future evolution of requirements: Rising customer requirements

Right now, "security is [perceived as] a supporting or enabling function" [I-1] in business - the same way as privacy. As described before, that leads to security and privacy being necessary areas where money is only spent but not created. The areas of security and privacy were, in the past, very strongly driven by compliance considerations. In contrast to that, nowadays, we see increasing customer requirements, which more and more succeed the baseline of protection that laws define. That being said, we can imagine an upcoming change in how security and privacy will be perceived:

This evolution could be a business opportunity if products fulfill more security or privacy requirements than necessary for compliance - which is already often the case. In analogy to already existing terms, companies could gain an advantage over competitors by offering security as a feature (or privacy as a feature). [4]

There are several business cases where customers might prefer - otherwise similar - solutions just because they have further security and privacy measures implemented. One example of this is having all data processing facilities inside the EU. Such requests are already being reported from some companies' sales departments according to [I-4], and we can imagine a continuation of their numbers growing.

If there will be actions towards a more secure and private product remains, of course, a management strategy decision. Implementing measures to increase the security and privacy of solutions is an investment - but we think that it is one that is worth it. We also imagine this will be done increasingly as the management's attitudes towards security and privacy change. From a business side, the implemented measures can ensure not only that products remain allowed to be sold and check the requirement list of customers but also create new business by attracting additional customers with further demands. Security and privacy might evolve from an area where money is only spent into an additional feature that can generate profits due to increased sales.

8.1.4. Security Implications on Privacy

First, we want to reason why our evaluation was very strict. In most cases where we criticized the data minimization conflict, the recorded data is only accessible by security departments or administrators. While this does not pose a threat, if those (often separate and maybe less protected) systems are breached, attackers could utilize that data. Examples of this

[3] This makes sense, as the governments primary interest is to maintain social stability and safety of its citizens. Paramount to keeping *resilience* is ensuring the basic needs of citizens can be met by protecting critical infrastructure. A analogy to this from the business world is *Business Continuity Management*.

[4] We gained a lot of positive feedback for this approach, especially from I-1. He even mentioned that he would "use this during the next security budget discussions".

were already included; one of the worst cases would be the breach of a phishing simulation tool, which is configured in a way that stores the passwords that employees enter during its awareness campaigns. Often, this data that the security measure creates is not even necessary for providing security, and the threat of it being abused could be eliminated by enforcing data minimization techniques in the first place.

However, sometimes, there is no easy way of solving the conflicts, which means that a compromise between security and privacy is necessary. One example is security cameras that surveillance and thereby increase security. This material could also be used negatively to violate privacy by connecting this video with user data and analyzing behavior patterns. Analog, this is the case for information security measures as well. To prevent this, we suggest either pseudonymizing or, if possible, anonymizing collected data (e.g., IP addresses) and only deanonymizing when necessary (e.g., in case of an incident investigation).

We want to mention here that - at least from the side of ISO - security frameworks have started to integrate more and more privacy aspects (and controls) within them. For example, the ISO control *8.11 Data masking* was added within the latest version of the ISO/IEC 27002 framework and could also be part of a data privacy framework. If this trend continues, and privacy and security grow even further together, it remains to be seen. To continue this scenario, this mixture between the different protection goals of security and privacy might continue and end in blending both topics, including merged confidentiality and secrecy. Meanwhile, an opposite pool could form that follows from the recent availability-centered security regulations.

To summarize, privacy principles like the data minimization approach should be applied to security measures when possible. Access to the created data should be strictly regulated to reduce the risk of privacy loss caused by security measures. This starts with enforcing the principle of least privilege to that data and can be extended to applying further measures that prevent a confidentiality loss in case of unauthorized access, e.g., by encrypting that collected data or pseudonymizing it.

Another finding already discussed in section 8.1.1 is that many synergies arose when the confidentiality aspect of security was the priority. This is because privacy's *secrecy* and security's *confidentiality* share synergies. Areas where conflicts were identified often focused on other security protection goals more.

8.1.5. Privacy handling in Practice

Even though the GDPR and other privacy regulations raise the importance of privacy protection, the practical implementation still needs improvement.

I-1 noted that "[p]rivacy makes us all liars. We click 'I have read and accepted' a hundred times, but no one really does. [...] It still needs to be sensibly implemented from my perspective." [I-1] Reasons for that are not only the "way too long texts that nobody reads or even understands". [I-6] The sheer number of consents and cookies "leads to the whole topic being despised, and it means that no one pays attention anymore." [I-1]

Terrible practical implementations of otherwise good intended privacy regulations lead

to counterproductive results. I-1 mentioned that he could not include "important security note[s]" anymore because people will ignore it and maybe "not [even] read that because they think 'there is again another privacy consent required'".

Another evolution in contrast to this - or maybe even a result of it - is the phenomenon of data dumping. I-6 mentioned that "there is the completely opposite type of people who photograph everything and share it on Instagram". I-5 criticized that for "customers [5], especially young people, it seems like the topic of data privacy is becoming less and less important. They prioritize the convenience that comes with being able to do things on social media without much thought" on privacy concerns.

Another problem he proposed was that even some employees already tried to circumvent certain parts of company-intern privacy regulations because they "simply no longer see the privacy restrictions as valid. [They] recently had a case involving the use of a cloud service hosted in China, which was not allowed according to [their] company policies. However, the customer still attempted to use it because it was a very convenient program, even after [I-5 had] informed them that their request had been rejected in the software registration process." [I-5]

It seems that there is a vast gap between the perceived value of privacy between customers on the one, and companies and jurists on the other side.

8.1.6. Use of PETs as a solution to security

Some PETs can help find solutions for security and privacy conflicts (e.g., anonymization and pseudonymization) – but not all PETs are suitable. We feel that applying specific PET characteristics as a feature to existing security solutions can solve most of the identified conflicts rather than integrating whole PETs.

Nevertheless, there are many interesting use cases where PETs could also be utilized in the context of security measures. Some examples are given in section 7.4, but further research could explore more.

Having already mentioned one suggestion for future work, we now transition to the last part of the discussion chapter.

8.2. Limitations and future work

The goal was to find an overview of overlapping areas between security and privacy. We would argue that by following a security framework, we had a structured approach containing most information security topics. While the level of completeness of the results, to identify and include every overlap between these two complex concepts, is impossible to determine, our approach reduced the uncertainty as best as possible.

[5] To clarify: In this section the word 'customer' refers to individuals, not to companies, like in the rest of this thesis.

One limitation is that this thesis only analyzed one security framework for its privacy implications. While different frameworks may contain slightly other controls, we would argue that the overlap between those frameworks is very high. By following the ISO/IEC 2700X standards, which are internationally being used, we think this covers the biggest part.

While different frameworks handle privacy differently than the ISO/IEC 2700X standards, a deeper evaluation of multiple frameworks was out of the scope of the thesis. However, future research could dive deeper into how different frameworks handle the interplay of security and privacy.

In particular, to focus the research around another framework, like the NIST Special Publication 800-53 [16], which already includes security and privacy controls, would be interesting. To investigate the privacy impact of its security controls and vice versa might reveal further insights.

One of our initial ideas was to compare the additions that the ISO/IEC 27701 framework proposes to our ISO measure analysis. We decided against this option due to the difference in versions described in chapter 2.2. One possible future work could further investigate our results in the context of the - yet unreleased - upcoming ISO/IEC 27701 standard.

Also, our approach starts by looking from the information security perspective and following a security framework to find possible implications for privacy. Further research could approach this topic from the privacy side, e.g., by starting with privacy principles and investigating their impact on security.

Other limitations include *researcher bias*. Because the manual secession of sources in the SLR could significantly impact the results, we tried to minimize this possibility by conducting expert interviews and a feedback workshop. These could validate and extend the previous results. One exclusion from this are the results in Chapter 6. Due to the extensive content of the interviews, or their backgrounds [6], we had to shorten or skip this part often during the interviews, as we needed to prioritize between getting better insight into the viewpoint of the experts and validating these results. Further research is needed to increase the reliability of these data.

In that frame, the next limitation arises due to the size of the *interviewee pool*. We would argue that the number of conducted interviews is sufficient and ensures enough diversity because the interviewees were from four companies. While three interviewees were from the same company, two of them joined that company just recently (within the last half year prior to the interview). Also, the interviewees were professionals with a combined working experience of over 107 years. We also included the feedback workshop to further increase the collected data's reliability. Some interviewees referred us to further experts, who unfortunately could not participate due to time constraints. Because the interviews included a lot of validation work that required mature content, the timeline of the thesis only allowed the

[6]Only half of the information security professionals did have experience in working with ISO controls in detail. This is because information security is a very large topic, with experts specializing in certain fields. In many projects external experts and consultants are hired, also when it comes to (ISO) certifications. Nevertheless, we still could address the areas where our findings are, e.g., also in the discussion around privacy in development projects with I-6.

interviews to be performed during the summer holiday season, during July and early August. Therefore, further validation work, mainly focusing on chapters 6 and 7, could extend the validity and generalizability of the results while discovering further use cases for PETs.

9. Conclusion

RQ1: What are the definitions of security and privacy, and how are these concepts related in theory?

Security can be defined clearly by its three (main) protection goals:

- Confidentiality
- Integrity
- Availability

Privacy, on the other hand, has multiple perceptions, resulting in many different definitions. We instead describe privacy by six overlapping *similarities*, which were identified by Solove: [13]

- The Right to Be Let Alone
- Limited Access to the Self
- Secrecy
- Control Over Personal Information
- Personhood
- Intimacy

While both concepts include *confidentiality* - or *secrecy* as the privacy side calls it - the difference is the scope. Because security protects all data, privacy can be seen as a security subsection covering only PII.

But other goals of privacy also exceed security, making it a separate yet closely related concept: There are *"privacy-specific" aspects*, which include various privacy principles, e.g., *data minimization* or *purpose limitations*.

These, including further findings, are visualized in the *concept map*. While the *general concept map* includes an overview, details are contained in the snapshots of the corresponding dimensions. [1]

[1] *General concept map* in Figure 5.11.
Definitions in Figure 5.1,
Protection Goals in Figure 5.2,
Requirements in Figure 5.3,
Frameworks in Figure 5.4, and
Measures in Figure 5.5.

RQ2: From the viewpoint of information security experts, how do the concepts of security and privacy overlap in practice, and what are possible conflicting requirements or synergies?

The experts confirmed the results from RQ1, and their feedback helped to extend the concept map.

The general relationship follows the identified differences and overlaps:

- I-1 mentioned the context of confidentiality, where security has a "supporting or enabling function for privacy."
- But they also often have conflicting requirements, which makes "[b]alancing the need for security measures with preserving privacy [...] a delicate task". [I-2]

To further investigate those *conflicting requirements*, we developed a process. Therefore, we started by modeling one current process for privacy impact evaluation (Figure 6.1). We ended with a three-layer decision tree (Figure 6.2) that we then used to evaluate the privacy implications of security measures. [2]

- We could identify a total of 30 possible conflicts:
  5.9, 5.11, 5.14, 5.15, 5.16, 5.17, 5.24, 5.26, 5.28, 5.31, 5.33, 6.1, 6.3, 6.4, 7.2, 7.4, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.13, 8.15, 8.16, 8.20, 8.21, and 8.23
- 36 synergies were found (with the first three being indirect):
  5.3, 5.5, 5.6, 5.10, 5.13, 5.14, 5.15, 5.16, 5.17, 5.18, 5.20, 5.23, 5.24, 5.26, 5.32, 5.33, 5.34, 6.6, 6.7, 7.7, 7.10, 7.14, 8.1, 8.2, 8.3, 8.4, 8.5, 8.10, 8.11, 8.12, 8.15, 8.24, 8.26, 8.27, 8.31, and 8.33
- We recognized that in 6 areas, synergies were possible:
  5.8, 5.12, 5.19, 5.21, 5.31, and 6.2

RQ3: To what extent can PETs fulfill information security requirements to replace information security measures in certain areas?

To precisely answer the question, PETs are designed for very specific use cases. If that matches with security requirements, they could indeed replace them. However, it is more likely that the security measure would instead change and adopt the PETs rather than be replaced by them. It can be argued whether that counts as PETs replacing information security measures.

Our approach to finding solutions to the identified conflicts might help as an initial basis to explore if PETs could be used in these cases.

- 20 of the possible conflicts were identified as solvable:
  5.9, 5.11, 5.15, 5.16, 5.17, 5.24, 7.2, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.15, 8.16, 8.20, 8.21, and 8.23

[2] To be precise, we followed the ISO/IEC 27001 annex controls, which are described in detail in ISO/IEC 27002. [9]

- Five did contain solvable parts:
  5.26, 5.28, 6.1, 6.3, and 7.4
- Five conflicts were found that are not solvable:
  5.14, 5.31, 5.33, 6.4, and 8.13

In particular, *pseudonymization* and *anonymization* techniques helped to achieve this. We also discovered further use cases of PETs that require more investigations.

- Zero-Knowledge Proofs
- Trusted execution environments
- Pseudonymization
- Synthetic data

In conclusion, we could differentiate between security and privacy and identify their perceptions and goals. The concept map provides a broad overview of the most important aspects of both concepts. The ISO controls analysis revealed several overlaps but also some areas of conflict that should be considered carefully. Our approach to utilizing privacy techniques like pseudonymization or anonymization can further help to achieve security while maintaining privacy.

A. General Addenda

A.1. Interview Questionnaire

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?

Definitions
3. How would you **define security?**
4. How would you **define privacy**?

General Relationship between Privacy and Security
5. How do you view the **general relationship** between security and privacy?
   - What are the **main differences and overlaps** between security and privacy?
   - Are they **conflicting or complementary**?
   - Can you think of examples where they have **conflicts**?
   - Can you think of examples where they have **synergies**?
6. Does this **overview of the concept map** represent the relationship as you view it?
7. Does this **concept map** show the most important aspects of the relationship?

Privacy/Security in Practice
8. What role does privacy/security play in your **work**?
   - Do you think privacy/security will become a **bigger concern**?
9. How do you **collaborate** with other departments regarding privacy/security topics?
   - Do you think the **responsibilities** of privacy/security topics will shift to other departments? (If yes, where?)
10. What are the **biggest challenges** or threats to privacy/security that you are confronted with in your work?

ISO Measures
11. What do you think of the **approach**?
12. What would you change/evaluate **differently**?
13. How did you deal with those **conflicts**?
    - Which **situations** did you experience where prioritizing security measures might compromise privacy, or vice versa?
    - What are the considerations to find the right **balance** between privacy and security measures?

PETs (Privacy Enhancing Technologies)
14. Are you familiar with PETs?
15. Do you use PETs? (If yes, which?)
16. Do you think PETs could replace the need for some security measures in some areas? (e.g., privacy by design)

Looking Forward
17. Is there anything else you would like to **add** regarding privacy and security?
    - Do you have any **additional insights** you would like to share?
    - Is there any aspect of this topic we may have **missed**?
18. Can you **refer** anyone who would also be able to contribute to this discussion?

A.2. Interview Translations

Some of the interviews were conducted in German. In order to directly quote them in this thesis, we translated these answers. The table below includes the translations besides their original German version, as well as the code of the interviewee.

Interviewee	Original Quote	Translated Quote
I-1	Also eigentlich ist Privacy zum Schutz der personenbezogenen Daten da. Das bedeutet, dass meine Daten so geschützt werden, wie ich mir das wünsche. Oder auch von Kunden oder von allen Individuen.	Privacy is actually about protecting personal data. It means that my data should be protected the way I want it to be. Or the data of customers or individuals in general.
I-1	Ja, also der Cyber Resilience Act kommt ja noch. Das wird 2026 noch ein großes Thema.	Yes, the Cyber Resilience Act is also upcoming, and that will be a significant topic in 2026.
I-1	Sicherheit ist Unterstützer Funktion oder Enabler des Datenschutzes in der digitalen Welt.	Security is a supporting or enabling function for privacy in the digital world.
I-1	Das Problem ist eben, dass man theoretisch auch ohne Incident in die Daten reingehen könnte.	The problem is, that in theory the data could also be accessed also without an incident.
I-1	Das [security as a feature] ist eine sehr gute Idee. Ich denke das nehme ich als Argument für die nächste Budget-Runde mit.	That [security as a feature] is a very good idea. I think I might even use this during the next security budget discussions.
I-1	Privacy macht uns alle zu Lügnern. 100 mal klickst du auf, ich habe es gelesen und akzeptiert. [...] Es muss noch sinnvoller implementiert werden. Aus meiner Sicht.	Privacy makes us all liars. We click "I have read and accepted" a hundred times, but no one really does. [...]It still needs to be sensibly implemented from my perspective.
I-1	Data Primary, so wie sie im Moment implementiert ist, mit diesen Millionen Zustimmungen, einer Milliarde Cookies, das führt dazu, dass dieses ganze Themengebiet nur noch verachtet wird und führt dazu, dass keiner mehr irgendetwas anschaut. Also meiner Meinung nach ist das absolut kontraproduktiv, absolut negativ.	Data privacy, as it's currently implemented, with these millions of consents, a billion cookies, it leads to the whole topic being despised, and it means that no one pays attention anymore. In my opinion, it's absolutely counterproductive, absolutely negative.

Interviewee	Original Quote	Translated Quote
I-1	Wenn du dann mal einen wichtigen Security Hinweis machen möchtest – das liest dann keiner mehr, weil jeder wieder glaubt, das ist wieder so eine data privacy Zustimmung nötig.	If you want to make an important security note - people will not read that, because they think, there is again another privacy consent required.
I-1	Ja klar, würde ich schon jetzt sagen. Weil wir haben ja nicht nur confidentiality, sondern auch integrity und availability. Und wir haben auch confidential data, die außerhalb von personenbezogenen Daten sind.	Yes, of course, I would say so already. Because we have not only confidentiality but also integrity and availability. And we also have confidential data that is separate from personal data.
I-5	Datenschutz ist für mich der verantwortungsvolle Umgang von Daten, insbesondere von personenbezogenen und sensiblen Daten, die mehr schützenswert sind.	Privacy is for me the responsible handling of data, in particular personal and sensitive data, which need more protection.
I-5	[...] für Kunden, vor allem Jugendliche, wird das Thema Datenschutz immer unwichtiger habe ich das Gefühl. Die Priorisieren den Komfort, den es mit sich bringt, wenn man ohne viel zu überlegen einfach etwas bei Social Media machen kann.	[...] for customers, especially young people, it seems like the topic of data privacy is becoming less and less important. They prioritize the convenience that comes with being able to do things on social media without much thought.
I-5	Manche Kunden sehen die Datenschutzeinschränkungen auch einfach nicht mehr ein. Wir hatten erst neulich einen Fall, in dem es um die Nutzung einer Cloud ging, die in China gehostet war und daher nach unseren Firmenrichtlinien nicht erlaubt war. Der Kunde hat aber trotzdem versucht, das zu nutzen, da es ein sehr komfortables Programm ist, selbst nachdem ich ihm rückgemeldet habe, dass sein Antrag im Softwareregistrierungsprozess abgelehnt wurde.	Some customers simply no longer see the privacy restrictions as valid. We recently had a case involving the use of a cloud service hosted in China, which was not allowed according to our company policies. However, the customer still attempted to use it because it was a very convenient program, even after I informed them that their request had been rejected in the software registration process.

Interviewee	Original Quote	Translated Quote
I-5	Nein, ich glaube nicht, dass es überhaupt vollständigen Datenschutz gibt – genauso wie es keine vollständige Sicherheit gibt, da nie garantiert werden kann, dass Daten nicht mehr rekonstruierbar sind oder deanonymisiert werden können. Man muss sich nur den Fortschritt der Technik ansehen, was für Leistungen heutzutage Prozessoren leisten – damit kann man heute bruteforcen, was noch vor wenigen Jahren unvorstellbar war – und Quantencomputing wird alles auch nochmal gänzlich verändern.	No, I don't believe that there is complete data privacy at all – just as there is no complete security, as it can never be guaranteed that data cannot be reconstructed or deanonymized. One only needs to look at the progress of technology and what processors can achieve today – they can nowadays perform bruteforce attacks on what was unimaginable just a few years ago – and quantum computing will completely change the game as well.
I-6	Ja, das können wir sagen. Also, ich glaube schon, dass immer noch ein gewisses Maß an Sicherheit erforderlich ist, insbesondere während der Übertragung. Wenn ich beispielsweise sage, der Shop läuft nur auf HTTP anstelle von HTTPS, selbst wenn die Daten nicht gespeichert werden, würden sie immer noch unverschlüsselt über das Netzwerk übertragen. Jemand könnte sie möglicherweise durch einen Man-in-the-Middle-Angriff abfangen. Wir müssen berücksichtigen, dass sie überhaupt nicht gespeichert werden. Wenn ich zum Beispiel sage, ich weiß nicht, ein Online-Shop, erstellt er am Ende immer noch eine Rechnung. Bestimmte Dinge müssen aufbewahrt werden. Man kann nicht einfach behaupten, dass die Rechnung des Online-Shops danach vollständig verschwindet.	Yes, we can say that. So, I do believe that a certain level of security is still needed, especially during transmission. For example, if I were to say the shop is running on HTTP instead of HTTPS, even though the data might not be stored, it would still be transmitted over the network without encryption. Someone could potentially intercept it through a man-in-the-middle attack. We have to consider that they are not stored at all. So, if I say, for instance, I don't know, an online shop, it still generates an invoice at the end. Certain things must be retained. You can't just claim that the online shop invoice disappears completely afterward.
I-6	Sozusagen, dass ich Herr meiner Daten bin.	So to say, that I'm master of my data.

Interviewee	Original Quote	Translated Quote
I-6	Ja, das würde ich sagen. Gesetzliche Vorgaben erfordern es, weißt du. Du musst Buchhaltung machen, vielleicht Steuererklärungen abgeben, eine Bilanz erstellen und all das Zeug brauchst du. Also, ich meine, es mag ein schöner Gedanke sein zu sagen, man sammelt oder speichert nichts, aber du benötigst trotzdem ein gewisses Mindestmaß an Verarbeitung und tatsächlich auch Speicherung. Daher ist auch ein gewisses Maß an Sicherheit erforderlich. Es ist also nicht etwas, das du vollständig weglassen kannst, da habe ich meine Zweifel. Vielleicht, wenn du keine Datenbank zur Speicherung benötigst, musst du dir keine Gedanken darüber machen, ob die Datenbank sicher ist oder nicht. Aber andererseits kannst du Ansätze wählen, bei denen du versuchst, so wenig wie möglich zu speichern und zu verarbeiten, und dich dann auf die Sicherheit in diesem speziellen Bereich konzentrierst oder sie zumindest herunterschaltest. Ich glaube, das ist möglich, aber zu sagen, dass du überhaupt keine Sicherheit brauchst, dass du deine Tür weit offen lässt oder dass du metaphorisch gesprochen keine Verschlüsselung während der Übertragung benötigst, das kann ich mir jetzt nicht wirklich vorstellen.	Well, you see, certain things are necessary, I'd say. Legal requirements, you know, require it. You have to do accounting, maybe file tax returns, prepare a balance sheet, and you need all that stuff. So, I mean, it might be a nice thought to say you don't collect or store anything, but you still need a certain minimum level of processing, and in fact, storage. Hence, you also need a certain level of security. So, it's not something you can entirely do away with, I have my doubts. Maybe if you don't need a database to store things, you don't have to worry about whether the database is secure or not, but then again, you can choose approaches where you try to store and process as little as possible, and then focus on security for that specific area, or at least scale it down. I believe that's possible, but saying that you don't need any security at all, that you leave your door wide open, or that, I mean, metaphorically speaking, you say you don't need encryption during transmission, I can't quite imagine that now.
I-6	Aus einem Risiko heraus entsteht unter Umständen ein Requirement, das wiederum zu einer Measure führt, die dann dafür dient, um die Protection Goals zu erreichen.	A requirement may arise from a risk, which in turn leads to a measure that serves to achieve the protection goals.

Interviewee	Original Quote	Translated Quote
I-6	Diese [Geschäftsbedingungen] sind viel zu lange Texte die niemand liest oder selbst wenn, nicht versteht.	Those are way too long texts, that nobody reads or even understands.
I-6	Und dann gibt es noch mal komplett die andere Seite, die wirklich von allem Fotos machen und auf Instagram oder was weiß ich teilen.	And then there is the completely opposite type of people who photograph everything and share it on Instagram, or I don't know.

A.3. Results of ISO control analysis

The following pages contain the results of the privacy impact analysis from chapter 6. The Control IDs and control names are adapted from the ISO/IEC 2700X controls. [9]

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which; If no, are there synergies)	Is the conflict solvable? (If yes, how)
5.1	Policies for information security	No		
5.2	Information security roles and responsibilities	No		
5.3	Segregation of duties	No, indirectly	No: Indirect synergies as foundations to role-based access and least privilege principles (5.15)	
5.4	Management responsibilities	No		
5.5	Contact with authorities	No, indirectly	No: Indirect synergies as privacy breaches also need to be reported and process could be synchronized	
5.6	Contact with special interest groups	No, indirectly	No: Indirect synergies (analog to 5.5)	
5.7	Threat intelligence	No		
5.8	Information security in project management	Yes, all kind of data within projects	No: Synergies possible by combining security assessment and privacy assessment in project management, including information determination and classification (5.12)	
5.9	Inventory of information and other associated assets	Yes, names	Yes: Data Minimization (names of information- and asset owners)	Yes, pseudonymize metadata
5.10	Acceptable use of information and other associated assets	Yes, all kind of data	No: Synergies with Purpose Limitation and Accountability	

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
5.11	Return of assets	Yes, names and metadata	Yes: Data Minimization (names who possess assets and location tracking of assets)	Yes, pseudonymize metadata, Partly: Change tracking from permanently to necessary
5.12	Classification of information	Yes, all kind of data	No: Synergies possible by including privacy category in information classification	
5.13	Labelling of information	Yes, all kind of data	No: Synergies dependent if intellectual property falls under definition of personal data	
5.14	Information transfer	Yes, all kind of data	No: Synergies with Secrecy and DPAs Yes: Data Minimization (contacts related to transfer)	No
5.15	Access control	Yes, all kind of data	Yes: Data minimization (Logging) No: Synergies by enforcing need-to-know / need-to-use principle and least-privilege principles, as assurance for purpose limitation and data minimization, and Secrecy	Yes, pseudonymize metadata
5.16	Identity management	Yes, names	Yes: Data Minimization (names) No: Synergies with Accountability, Transparency, and Secrecy	Yes, pseudonymize names
5.17	Authentication information	Yes, biometric data	Yes, Limited Access to the Self (only if biometric authentication is mandatory) No: Synergies with Secrecy	Yes, leave alternatives to biometric authentication
5.18	Access rights	No, indirectly	No: Synergies with Transparency and Secrecy	

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
5.19	Information security in supplier relationships	Yes, all kind of data	No: Synergies possible by also considering privacy of suppliers	
5.20	Addressing information security within supplier agreements	Yes, all kind of data	No: Synergies by also considering privacy in supplier agreements (e.g., DPAs)	
5.21	Managing information security in the ICT supply chain	Yes, all kind of data	No: Synergies possible by also considering privacy of supply chain	
5.22	Monitoring, review and change management of supplier services	Yes, all kind of data	No specific overlap.	
5.23	Information security for use of cloud services	Yes, all kind of data	No: Synergies, as PII protection should be considered	
5.24	Information security incident management planning and preparation	Yes, all kind of data	Yes: Data Minimization (Monitoring, Detection, Analyzing, Evidence collection, Root cause analysis) No: Synergies with Transparency (logging of incident management activities)	Yes, pseudonymize metadata
5.25	Assessment and decision on information security events	No		
5.26	Response to information security incidents	Yes, all kind of data	Yes: Data Minimization (Evidence collection, Forensic analysis, Root cause analysis) No: Synergies with Transparency (Logging of incident response activities)	Partly, pseudonymize metadata, but no, if necessary in legal case
5.27	Learning from information security incidents	No		

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
5.28	Collection of evidence	Yes, all kind of data	Yes: Data Minimization (Evidence collection, Forensic analysis, Root cause analysis), Data Retention (data stored for legal cases)	Partly, pseudonymize metadata, but no, if necessary in legal case
5.29	Information security during disruption	No		
5.30	ICT readiness for business continuity	No		
5.31	Legal, statutory, regulatory and contractual requirements	Yes, all kind of data	Yes: Cryptography (Legal requirements restrict usage) No: Synergies possible by including privacy laws	No
5.32	Intellectual property rights	Yes, intellectual property	No: Synergies dependent if intellectual property falls under definition of personal data	
5.33	Protection of records	Yes, all kind of data	Yes: not control itself, by but keeping records (that include PII) No: Synergies, as records should be kept secret and encryption is recommended (8.24)	Partly, encrypt data
5.34	Privacy and protection of PII	Yes, PII	No: Synergies due to PII protection for compliance with regulations, recommendation of privacy officer, Accountability	
5.35	Independent review of information security	No		

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
5.36	Compliance with policies, rules and standards for information security	No		
5.37	Documented operating procedures	No		
6.1	Screening	Yes, PII	Yes: Data Minimization (Collection of employee data, but with consideration of privacy regulation), Personhood (too extensive screening, prejudices)	Partly, involves use cases for Zero-Knowledge-Proofs
6.2	Terms and conditions of employment		No: Synergies possible by including privacy principles	
6.3	Information security awareness, education and training	Yes, names and metadata	Yes: Data Minimization (names)	Partly, pseudonymize metadata
6.4	Disciplinary process	Yes, names	Partly: Control demands protection of name of perpetrators,	No
6.5	Responsibilities after termination or change of employment	No		
6.6	Confidentiality or non-disclosure agreements	Yes	No: Synergies (Secrecy)	
6.7	Remote working	Yes	No: Synergies (Secrecy)	
6.8	Information security event reporting	No		
7.1	Physical security perimeters	No		

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
7.2	Physical entry	Yes, names and biometric data	Yes: Data Minimization (physical logbook of all access), Limited Access to the Self (biometric authentication, inspection and examination of personal belongings)	Manual: No Digital: Yes, pseudonymize metadata, leave alternatives to biometric authentication
7.3	Securing offices, rooms and facilities	No		
7.4	Physical security monitoring	Yes, recordings	Yes: Data Minimization (surveillance in accordance to data protection laws)	Partly, anonymize metadata / blur faces
7.5	Protecting against physical and environmental threats	No		
7.6	Working in secure areas	No		
7.7	Clear desk and clear screen	Yes, all kind of data	No: Synergies (Secrecy)	
7.8	Equipment siting and protection	No		
7.9	Security of assets off-premises	Yes, names and metadata	Yes: Data Minimization (names by logging of custody, location tracking of devices)	Yes, pseudonymize metadata
7.10	Storage media	Yes, all kind of data	No: Synergies (Secrecy, by promoting cryptographic techniques)	
7.11	Supporting utilities	No		
7.12	Cabling security	No		
7.13	Equipment maintenance	No		
7.14	Secure disposal or re-use of equipment	Yes, all kind of data	No: Synergies (Secrecy, Cryptography)	

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
8.1	User endpoint devices	Yes, metadata	Yes: Data Minimization (end user behaviour analytics 8.16) No: usage of privacy screen filters, consider PII protection laws in the BYOD context	Yes, anonymize metadata
8.2	Privileged access rights	Yes, names and metadata	No: Accountability Yes: Data Minimization (record of all privileges allocated)	Yes, pseudonymize metadata
8.3	Information access restriction	Yes, metadata	No: Accountability (no anonymous access) Yes: Data Minimization (monitor the use of the information, no anonymous access)	Yes, anonymize metadata
8.4	Access to source code	Yes, metadata	No: Accountability (log accesses and of all changes to source code) Yes: Data Minimization (log accesses and of all changes to source code)	Yes, pseudonymize metadata
8.5	Secure authentication	Yes, metadata and biometric data	No: Accountability Yes: Data Minimization (logging unsuccessful and successful attempts) and Limited Access to the Self (biometric authentication)	Yes, pseudonymize metadata, leave alternatives to biometric authentication
8.6	Capacity management	Yes, metadata	Yes: Data Minimization (Monitoring)	Yes, anonymize metadata
8.7	Protection against malware	Yes, metadata	Yes: Data Minimization (Scanning of all incoming traffic, as well as webpages)	Yes, pseudonymize metadata
8.8	Management of technical vulnerabilities	No		
8.9	Configuration management	No		

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
8.10	Information deletion	Yes, all kind of data	No: Synergies with data retention and secrecy	
8.11	Data masking	Yes, all kind of data	No: Synergies (Secrecy by PII masking)	
8.12	Data leakage prevention	Yes, all kind of data	No: Synergies (Secrecy by PII protection)	
8.13	Information backup	Yes, all kind of data	Yes: Data retention (right to erasure)	No
8.14	Redundancy of information processing facilities	No		
8.15	Logging	Yes, metadata	Yes: Data Minimization (Logging) No: Synergies (Accountability)	Yes, dependent on use anonymize or pseudonymize metadata
8.16	Monitoring activities	Yes, metadata	Yes: Data Minimization (Analysis and documentation)	Yes, pseudonymize metadata
8.17	Clock synchronization	No		
8.18	Use of privileged utility programs	No	(Out of scope, as only affects users of utility programs)	
8.19	Installation of software on operational systems	No		
8.20	Networks security	Yes, all kind of data	Yes, Data Minimization (Logging and monitoring)	Yes, pseudonymize metadata
8.21	Security of network services	Yes, meta data	Yes, Data Minimization (Monitoring)	Yes, pseudonymize metadata
8.22	Segregation of networks	No		

Control ID	Control Name	Is PII involved?	Is any privacy principle breached?	Is the conflict solvable?
8.23	Web filtering	Yes, all kind of data	Yes, Data Minimization (Monitoring)	Yes, dependent on use anonymize or pseudonymize meta-data
8.24	Use of cryptography	Yes, all kind of data	No, Synergies with secrecy (PII protection)	
8.25	Secure development life cycle	No		
8.26	Application security requirements	No	No, Synergies due to consideration of need for privacy	
8.27	Secure system architecture and engineering principles	Yes, all kind of data within projects	No, Synergies (encryption) already in place, could be extended (“privacy by design”, . . .)	
8.28	Secure coding	No		
8.29	Security testing in development and acceptance	No		
8.30	Outsourced development	No		
8.31	Separation of development, test and production environments	Yes, all kind of data within projects	No, Synergies with privacy: Secrecy (PII protection),	
8.32	Change management	No		
8.33	Test information	Yes, all kind of data within projects	No, Synergies with privacy (analog to 8.31)	
8.34	Protection of information systems during audit testing	No		

List of Figures

2.1. ISO/IEC 2700X standards, adapted from ISO/IEC 27000. [6] 5

3.1. Cybersecurity and Privacy Risk Relationship, adapted from the NIST privacy framework. [16] 9

4.1. The three key steps. 11
4.2. Overview of the different steps during the creation of this thesis. 19

5.1. Snapshot of the *definitions* dimension in the concept map. 27
5.2. Snapshot of the *protection goals* dimension in the concept map. 28
5.3. Snapshot of the *requirements* dimension in the concept map. 34
5.4. Snapshot of the *frameworks* dimension in the concept map. 35
5.5. Snapshot of the *measures* dimension in the concept map. 38
5.6. General view of the initial version of the concept map. 39
5.7. General view of the concept map with additions from the feedback workshop. 40
5.8. Detailed view of the *Requirements* and *Frameworks* dimensions of the concept map with additions from the feedback workshop. 40
5.9. Detailed view of the *Requirements* and *Frameworks* dimensions of the concept map with additions from the interviews. 41
5.10. General view of the concept map with the first additions from the interviews. 43
5.11. Final version of the general view of the concept map. 44

6.1. Evaluation of privacy considerations in companies. 46
6.2. Decision tree used to evaluate possible privacy impact of ISO 27001 controls. . 48

List of Tables

4.1. Databases used 12
4.2. Number of results based on keywords 13
4.3. Workshop Participants 15
4.4. Interview Partners 17

Acronyms

AICPA American Institute of Certified Public Accountants. vi, 29, 36

DPA Data Processing Agreement. 51, 52

GDPR General Data Protection Regulation. 1, 6, 8, 21, 25, 30–32, 34, 36, 39, 45, 49, 50, 53, 62, 69

ISMS Information Security Management System. 5, 6, 17, 34, 45, 49

ISO International Organization for Standardization. vi, 31, 34, 36, 69

KRITIS BSI Critical Infrastructure Regulation. 31, 33, 67

NIS Network and Information Security Directive. 31, 33, 67

NIST National Institute of Standards and Technology. vi, 9, 37, 38, 67

PET Privacy-Enhancing Technology. vi, 2, 6, 7, 10, 11, 16, 18, 19, 22, 62–66, 70, 72, 74, 75

PII Personal Identifying Information. 9, 21, 24, 25, 29, 36, 45–47, 49–51, 53–60, 62, 65, 67, 73

PIMS Privacy Information Management System. 6, 34, 49

RQ1 what are the definitions of security and privacy, and how are these concepts related in **theory**?. 1, 10, 12, 73, 74

RQ2 from the viewpoint of information security experts, how do the concepts of security and privacy overlap **in practice**, and what are possible conflicting requirements or synergies?. 1, 10, 74

RQ3 to what extent can **PETs** fulfill information security requirements to replace information security measures in certain areas?. 2, 10, 16, 19, 74

SLR systematic literature review. 11–14, 20, 30, 71

SOC Systems and Organization Controls. 29, 31, 36, 37

SPI Sensitive Personal Information. 47

Bibliography

[1] *Oxford Advanced Learner's Dictionary at Oxford Learner's Dictionaries*. URL: https://www.oxfordlearnersdictionaries.com/definition/english (visited on 08/22/2023).

[2] *Cambridge English Dictionary*. URL: https://dictionary.cambridge.org/dictionary/english-german/security (visited on 08/22/2023).

[3] A. Brockhaus. *IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit: Wo liegen die Unterschiede?* Nov. 2019. URL: https://www.is-its.org/it-security-blog/it-sicherheit-informationssicherheit-cyber-sicherheit-unterschiede (visited on 08/23/2023).

[4] National Institute of Standards and Technology (NIST). *NIST Glossary*. URL: https://csrc.nist.gov/glossary (visited on 08/22/2023).

[5] S. D. Warren and L. D. Brandeis. "The right to privacy". In: *Harvard Law Review* 4.5 (1890), p. 193. DOI: 10.2307/1321160.

[6] International Organization for Standardization. *ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary*. 2018.

[7] J. Ryerse. *Top 11 cybersecurity frameworks*. Feb. 2023. URL: https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks (visited on 08/20/2023).

[8] International Organization for Standardization. *ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. 2019. URL: https://www.iso.org/standard/71670.html.

[9] International Organization for Standardization. *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls*. 2022. URL: https://www.iso.org/standard/75652.html.

[10] *Regulation (EU) 2016/679 of the European Parliament and of the Council*. of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016. URL: https://data.europa.eu/eli/reg/2016/679/oj.

[11] Information Commissioner's Office (ico.) *Privacy-enhancing technologies (PETs)*. Version 1.0.5. June 2023.

[12] J. H. Moor. "Towards a theory of privacy in the information age". In: *ACM SIGCAS Computers and Society* 27.3 (1997), pp. 27–32. DOI: 10.1145/270858.270866.

[13] D. J. Solove. "Conceptualizing Privacy". In: *California Law Review* 90.4 (2002), pp. 1087–1155. ISSN: 00081221.

[14] E. Ventrella. "The symbiotic relationship between privacy and security in the context of the General Data Protection Regulation". In: *ERA Forum* 20.3 (Sept. 2019), pp. 455–469. DOI: 10.1007/s12027-019-00578-6.

[15] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-53 Revision 5*. Security and Privacy Controls for Information Systems and Organizations. Sept. 2020. URL: https://doi.org/10.6028/NIST.SP.800-53r5.

[16] National Institute of Standards and Technology (NIST). *NIST Privacy Framework*. A tol for improving privacy through enterprise risk management, version 1.0. Jan. 2020. URL: https://doi.org/10.6028/NIST.CSWP.01162020.

[17] B. Kitchenham and S. Charters. "Guidelines for performing Systematic Literature Reviews in Software Engineering". In: *EBSE Technical Report* (2007).

[18] D. Kudryavtsev and T. Gavrilova. "From Anarchy to System: A Novel Classification of Visual Knowledge Codification Techniques". In: *Knowledge and Process Management* 24.1 (2017), pp. 3–13. DOI: https://doi.org/10.1002/kpm.1509. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/kpm.1509.

[19] J. D. Novak and A. J. Cañas. "The Theory Underlying Concept Maps and How to Construct and Use Them". In: *Technical Report IHMC CmapTools 2006-01 Rev 01-2008* (2008). URL: http://cmap.ihmc.us/Publications/ResearchPapers/TheoryUnderlyingConceptMaps.pdf.

[20] T. George. "Semi-Structured Interview | Definition, Guide & Examples". In: *Scribbr* (June 2023). URL: https://www.scribbr.com/methodology/semi-structured-interview/ (visited on 08/18/2023).

[21] J. Gläser and G. Laudel. In: *Experteninterviews und qualitative inhaltsanalyse Lehrbuch*. VS Verlag, 2010. ISBN: 978-3-531-17238-5.

[22] J. Fantaye. *An Introduction and Overview of Privacy-Enhancing Technologies for Data Processing and Analysis*. [Bachelor's Thesis, Technical University of Munich]. 2023.

[23] ISACA. *ISACA Glossary*. URL: https://www.isaca.org/resources/glossary (visited on 08/22/2023).

[24] California Legislature. *Senate Bill No. 1121, California Consumer Privacy Act of 2018*. Accessed: Sep. 5, 2023. 2018. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

[25] International Association of Privacy Professionals (IAPP). *What is Privacy*. 2023. URL: https://iapp.org/about/what-is-privacy/ (visited on 09/05/2023).

[26] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications". In: *IEEE Internet of Things Journal* 4.5 (2017), pp. 1125–1142. DOI: 10.1109/JIOT.2017.2683200.

[27] G. E. M. Anscombe, R. Rhees, and G. H. Von Wright. *Philosophische Untersuchungen*. Reproduction of "Philosophische Untersuchungen" by L. Wittgenstein. 1999. URL: https://www.wittgensteinproject.org/w/index.php?title=Philosophische_Untersuchungen (visited on 09/01/2023).

[28] A. Biletzki and A. Matar. "Ludwig Wittgenstein". In: *The Stanford Encyclopedia of Philosophy*. 2021. URL: https://plato.stanford.edu/entries/wittgenstein/ (visited on 09/01/2023).

[29] D. J. Solove. "Nothing to Hide: The False Tradeoff Between Privacy and Security". In: (2011). URL: https://ssrn.com/abstract=3976770.

[30] R. Koch. *Cookies, the GDPR, and the ePrivacy Directive*. URL: https://gdpr.eu/cookies/ (visited on 09/05/2023).

[31] T. R. Nathalie Koch. *Cookies under attack – New decisions by European data protection authorities on online advertising*. Feb. 2022. URL: https://www.taylorwessing.com/en/insights-and-events/insights/2022/02/cookies-under-attack (visited on 09/05/2023).

[32] E. Godkin. *Libel and Its Legal Remedy*. 1880. URL: https://www.theatlantic.com/magazine/archive/1880/12/libel-and-its-legal-remedy/63221.

[33] K. A. Nelson. *Daniel Solove's six general types of privacy*. Dec. 2011. URL: https://inpropriapersona.com/articles/daniel-soloves-six-general-types-of-privacy/.

[34] T. Madiega and H. Mildebrath. *Regulating facial recognition in the EU*. Sept. 2011. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA%282021%29698021_EN.pdf.

[35] J. R. Vile. *Related cases in Privacy, Freedom of the Press: Department of Justice v. Reporters Committee For Freedom of the Press (1989)*. 2009. URL: https://mtsu.edu/first-amendment/article/1577/ (visited on 09/06/2023).

[36] A. Alowairdhi and X. Ma. "Data Brokers and Data Services". In: *Encyclopedia of Big Data*. Springer International Publishing, 2019. DOI: https://doi.org/10.1007/978-3-319-32001-4_298-1.

[37] U. S. Court. *505 U.S. 833, Planned Parenthood of Southeastern Pennsylvania v. Casey*. 1992.

[38] P. A. Lontsikh, V. A. Karaseva, E. P. Kunakov, I. I. Livshitz, and K. A. Nikiforova. "Implementation of information security and data processing center protection standards". In: *2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS)*. 2016.

[39] E. Bertino. "Data Security and Privacy: Concepts, Approaches, and Research Directions". In: *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 1. 2016, pp. 400–407. DOI: 10.1109/COMPSAC.2016.89.

[40] AICPA. *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Includes March 2020 updates. 2020. URL: https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria-2020.pdf.

[41] S. J. Ross. "Information Security Matters: Secrecy and Privacy". In: *ISACA Journal* (2020).

[42] P. Gröschler and L. Iking. "Folge 7: Lex specialis". In: *Latein für Juristen*. Johannes Gutenberg Universität Mainz, 2020.

[43] BaFin. *VAIT - Supervisory Requirements for IT in Insurance Undertakings*. Mar. 2022. URL: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_030822_VAIT_en.html.

[44] TÜV SÜD. *TISAX - Der Nachweis für IT-Sicherheit in der Automobilbranche*. URL: https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/tisax (visited on 08/31/2023).

[45] BSI. *Legal basis*. URL: https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Rechtsgrundlagen/rechtsgrundlagen_node.html (visited on 08/31/2023).

[46] *Directive (EU) 2022/2555 of the European Parliament and of the Council*. of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[47] Uniqkey. *WWho Does NIS2 Apply To?* Collection of publicly-sourced information of the "NIS2 Directive". URL: https://nis2directive.eu/who-are-affected-by-nis2/ (visited on 09/10/2023).

[48] Cloudflare. *What is the ePrivacy Directive?* URL: https://www.cloudflare.com/learning/privacy/what-is-eprivacy-directive/ (visited on 09/05/2023).

[49] Microsoft. *Microsoft Compliance*. URL: https://learn.microsoft.com/en-us/compliance/ (visited on 09/10/2023).

[50] Organisation for Economic Co-operation and Development (OECD). *Privacy*. URL: https://www.oecd.org/digital/privacy/ (visited on 09/10/2023).

[51] Asia-Pacific Economic Cooperation. *APEC privacy framework*. URL: https://learn.microsoft.com/en-us/compliance/ (visited on 09/10/2023).

[52] United Nations (UN). *68/167. The right to privacy in the digital age*. Resolution adopted by the General Assembly on 18 December 2013. 2022.

[53] G. P. Digital. *World map of encryption laws and policies*. URL: https://www.gp-digital.org/world-map-of-encryption/ (visited on 09/09/2023).

[54] Secureframe. *What is SOC 2?* URL: https://secureframe.com/hub/soc-2/what-is-soc-2 (visited on 09/09/2023).

[55] AICPA. *AICPA website*. URL: https://www.aicpa-cima.com/home (visited on 09/09/2023).

[56] A. Prozorov. *Best Privacy Standards and Frameworks*. Version 1,3. July 2023.

[57] M. Rosulek. *A Brief Overview of Private Set Intersection*. Presented at Special Topics on Privacy and Public Auditability (STPPA) series, event #2. Apr. 2021. URL: https://csrc.nist.gov/presentations/2021/stppa2-psi (visited on 08/30/2023).