Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance

Stephen Joseph Meisenbacher
Master’s Thesis in Informatics

Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance

Identifizierung praktischer Herausforderungen bei der Implementierung von technischen Maßnahmen für Datenschutz-Compliance

Author: Stephen Joseph Meisenbacher
Supervisor: Prof. Dr. Florian Matthes
Advisor: Oleksandra Klymenko, M.Sc.
Submission Date: 15.01.2022
I confirm that this master’s thesis in informatics is my own work and I have documented all sources and material used.

Munich, 15.01.2022

Stephen Joseph Meisenbacher
Acknowledgments

I really wanted to wait until the writing itself of this thesis was finished to complete this one last part; alas, as I sit here in the Munich airport on a cold November morning, far too early for my flight to Paris, I figured it would be an appropriate time to at least jot some things down. Hey, there’s no time like the present.

I would like to accomplish two things here, fully aware that this might not be the standard format of an acknowledgments section. I would firstly like to reflect briefly on the journey that has brought me to this point, namely one that I could have never imagined, and one that continues to unfold in weird and mysterious ways. As a “hybrid” American living in Munich and waiting for a flight to Paris, I cannot help be but reminded of this. Secondly, and more importantly, I would like to express my gratitude to those without whom I would literally not be here.

My meeting of a new person in Germany is almost undoubtedly met with the counter-question, “Why are you here?” The question is quite understandable; for a person like me to make the decision to study thousands of miles away, when there are “perfectly good” universities a stone’s throw away from my home, can be rather confounding. But back to the question, I usually resort to the straightforward “I received a scholarship”, or, in a more lighthearted manner, “I like Germany”.

The true answer to the question, though, can not and should not be answered so curtly; rather, the real story behind it results from a complex web of people, places, and happenings, one might say “at the intersection of Hard Work Avenue and Opportunity Boulevard”. I will not bore anyone with the details here. At this point, I would like to thank foremost my friends, classmates, teachers, professors, and advisors from St. Joe’s and Notre Dame – without you, there would be no foundation. In particular, to the friends that have for some reason stuck by me even when I’m halfway across the globe: you rock.

The decision to move to Germany did not come easy. On top of this, the adaptation to the German education system and all of its intricacies (whether that is used as an euphemism is up to you) did not by any means come easy. In short, it was a struggle. It is something that one must simply get used to, and I’m glad to say that I mostly got there. To my friends and colleagues in the Munich area, thank you, and sorry for always preferring English – I swear I can speak German.

Now comes for the actually relevant stuff. Right after a pretty darn tough first semester, both inside and outside the classroom, it became time to pull myself up by the bootstraps and do it all over again (for a second semester). It was at this relative point in time that two
things occurred: (1) that pesky little worldwide event starting with a co- and ending with a -rona, and (2) my random, seemingly menial decision to take a certain seminar named *Natural Language Processing: Methods and Applications*. Regarding (1), we won’t discuss. But the second event, however relatively unmeaningful at the time, would turn out to springboard a series of events that indeed shifted my life plan, quite literally.

Time for a second question that often came my way: “What will you do after Munich?”, or rather, “When are you coming back home?” Straight from the start of the Munich adventure, and up until fairly recently, this was in fact an easy question to answer: “Oh, after my Master’s, I’m going back, for sure!” Yet what started out as a random seminar choice turned into an incredible seminar experience, which turned into a challenging yet very fulfilling guided research semester, which quite seamlessly transitioned into this very thesis research, which will thereafter mark the beginning of my PhD studies at TUM. Oh, how wrong I was.

Now once again unreasonably early at the airport (CDG, return flight), it is now that I would like thank the fine people at TUM sebis for a few things. Firstly, for the seminar. Secondly, for the research opportunities, which not only served as an excellent (and arguably necessary) way to battle through the odd times of Corona, but more importantly for single-handedly forging my most current research interests. I came into this Master’s journey quite literally a novice, bursting with motivation but clearly lacking in true direction. Through my time so far with sebis, this has certainly changed. And on this note, I am incredibly grateful and humbled for the forthcoming research position – I look forward to the ups and downs, the challenges and (hopefully) successes. Specifically to Prof. Matthes: thank you for your belief in me! And finally, to my incredible advisor along this journey: Alexandra. Few will ever meet someone who handles an unbelievable workload so well, and still manages to provide valuable (and selfless!) guidance in the service of others. I owe much of my ever-growing knowledge on research practices, and all the fun stuff that comes along with it, to this single person. Many, many thanks!

Also a huge shout out and thank you to the interview and survey participants, without whom this thesis work would have absolutely no substance. Owing not as much as a response to a random stranger (me), these professionals went above and beyond, not only in taking their valuable time to assist in the research, but also in imparting their truly thought-provoking, genuinely insightful knowledge. In short, I hope one day to be able to do the same, and furthermore, to make a similar impact in the way that these people did for me.

Finally, for a second and hopefully not last appearance in the acknowledgements comes a heartfelt gratitude and appreciation for my family. While this time around was just a tad different from the ND days, you all continue to be my source of motivation, inspiration, consolation, and aspiration. I will restrain myself from writing more, both for its out-of-placeness but also the inadequacy to which any attempt to write further would amount. To Dad, Mom, Andrew, Brigid: thank you.

Okay, time to wrap this up. My true purpose in this thorough, possibly verbose, forward was to share a bit of the context surrounding the writing of this thesis, and moreover, the weird journey that led me to that point. It seems like yesterday that I was tearily writing my
way through the acknowledgments of my Bachelor Thesis, remarkably oblivious that I would even be doing something comparable again, let alone in Germany (more specifically in a Parisian airport). In light of this hopefully comprehensible but likely incomplete commentary on the complex journey that is life, I will sign off with a short quote that might just be the best way to leave things (and possibly could have just been inserted in lieu of this mini-novel):

I have fought the good fight, I have finished the race, I have kept the faith.
– 2 Timothy 4:7, NIV

And on this note, I invite you to read the following work that comprises my Master Thesis. I truly hope this it proves to be as interesting to you to read as it was for me to write. In what started out as a rather opaque, and honestly outright foreign, topic to me ended up as a wonderful exploration into a particular niche of our every-expanding interdisciplinary world, leading to many insights but also to clear avenues for further work and investigation. The following serves as my best attempt to contribute to the discussion, one that is of growing importance.

– SJM
18.11.21, Munich, Germany
20.11.21, Paris, France
05.01.22, Warren, NJ
Abstract

Recent years have seen the adoption of several data privacy protection laws, most notably the General Data Protection Regulation (GDPR) in the EU, the California Consumer Privacy Act (CCPA) in the United States, or even the lesser known Bundesdatenschutzgesetz in Germany. Legislation like the GDPR and CCPA shed light on an increasing worldwide awareness of the potential dangers and complications brought about by the ever-growing popularity of data collection, processing, and analysis. Furthermore, they represent an attempt to enforce the responsible handling of data through legal means, ultimately at its core protecting the consumer, or rather the individual. From these laws stems the concept of data privacy compliance, essentially meaning how a corporation or other organization must comply with the guidelines defined in such laws. At the same time, and in most cases actually predating these recent privacy laws, the research and development of Privacy-Enhancing Technologies (PETs) has also sharply risen, yielding many novel and effective methods for processing sensitive data in a private matter.

With two distinct sectors approaching the issue of data privacy in inherently different ways, one can reasonably expect challenges. Privacy in the legal sense, by nature, is more of a guideline rather than a specification. Advances in the technical realm, however, work towards developing processes that do indeed preserve privacy in some manner, yet this may or may not be directly translatable to given legislation. In other words, one can read through the entire text of the GDPR, yet still be unsure as to how this exactly could be implemented in a PET. By the same token, the developers of a PET might face challenges when evaluating how their framework conforms to GDPR guidelines. Thus, the goal of this thesis is not only to explore the dynamic existing between privacy compliance in the legal and technical sectors, but also to investigate the other challenges pervading the implementation of technical measures for privacy compliance. This goal will be accomplished by first exploring the challenges existing within privacy compliance programs today, and subsequently analyzing the findings to develop useful solutions.
## Contents

Acknowledgments iii

Abstract vi

1. Introduction 1

2. Foundations 3
   2.1. Privacy 3
      2.1.1. When Privacy is Threatened 4
   2.2. Privacy-Enhancing Technologies 5
   2.3. Regulation 6
      2.3.1. Privacy Regulation, A History 6
      2.3.2. European General Data Protection Regulation (GDPR) 7
      2.3.3. Others 9
   2.4. Important Definitions 9
      2.4.1. "Practical" 9
      2.4.2. "Challenges" 10
      2.4.3. "Technical Measures" 10

3. Related Work 11
   3.1. The Technical-Legal Gap 11
   3.2. Technical Measures 12
      3.2.1. Guidelines 12
      3.2.2. PETs 13
      3.2.3. Security 14
   3.3. Understanding Data Privacy, Compliance, and GDPR 14
      3.3.1. Past and Present Projects 15
      3.3.2. Organizations 15
   3.4. Privacy by Design 16
   3.5. Data Privacy and Society 17

4. Methodology 18
   4.1. Research Questions 18
   4.2. Methodology Design 19
      4.2.1. Qualitative Study: The Interview 19
      4.2.2. Quantitative Study: The Survey 21
5. The Interview Makeup 23
  5.1. Identifying Participants ........................................ 23
  5.2. Interviewee Demographics ................................. 25
    5.2.1. Experience .............................................. 25
    5.2.2. Gender .................................................. 28
    5.2.3. Location .................................................. 28
  5.3. The Interviewees, Summarized ............................ 29

6. The Structure of Privacy Compliance 32
  6.1. Definitions / Clarifications .................................. 32
    6.1.1. Organization .......................................... 32
    6.1.2. Talking About Compliance ............................ 32
  6.2. Roles and Responsibilities ................................ 33
    6.2.1. Legal .................................................. 33
    6.2.2. Technical ............................................... 35
    6.2.3. External Stakeholders ................................. 37
    6.2.4. The Go-Betweens ....................................... 38
  6.3. Interactions .................................................. 41
    6.3.1. Technical-Technical .................................. 41
    6.3.2. Technical-Legal ......................................... 42
    6.3.3. Legal-Legal .............................................. 43
    6.3.4. Documentation ......................................... 43
    6.3.5. Liability ................................................ 44
  6.4. The Privacy Compliance Structure, Visualized ............ 45
    6.4.1. The Diagram ............................................ 45

7. Challenges 47
  7.1. Setup .......................................................... 47
  7.2. The Technical-Legal Interaction ............................ 48
    7.2.1. Category Overview ...................................... 48
    7.2.2. The Challenges ......................................... 49
    7.2.3. Summary .................................................. 59
  7.3. Technologies .................................................. 59
    7.3.1. Category Overview ...................................... 60
    7.3.2. The Challenges ......................................... 61
    7.3.3. Summary .................................................. 75
  7.4. Organizational Factors ....................................... 76
    7.4.1. Category Overview ...................................... 77
    7.4.2. The Challenges ......................................... 77
    7.4.3. Summary .................................................. 90
  7.5. General ........................................................ 92
    7.5.1. Category Overview ...................................... 92
    7.5.2. The Challenges ......................................... 93
1. Introduction

We are living in the age of data. Whereas in the history of mankind, the discovery of powerful new tools such as bronze, iron, and finally steel undoubtedly propelled the course of the world forward, the modern “metal” now has taken a much more intangible form, under the umbrella term of data. In the way that steel revolutionized modern machinery, agriculture, and architecture, the harnessing of the power existing within data as we know it has enabled the rapid and advanced development of modern technologies. Indeed, it is quite difficult to ignore the quite tangible products of data-driven technology, with the ubiquity of social media and the like, but also with modern medicine, communication, and countless other developing fields. Without a doubt, data has created unprecedented business value and fostered countless marvelous new technologies.

One might argue that such advancement would be nearly impossible to have been achieved, and to continue to be achieved, without the utilization of massive datasets collected from a myriad of everyday sources, more often referred to as “big data”. At its core, the main premise and motivation behind this approach is the ability to gain powerful insight into patterns located within the data, perhaps those even imperceptible to a trained data analyst. In turn, such rich data can be used to create models with impressive predictive accuracy, and furthermore, ones that possess the ability to make everyday decisions. On the whole, the amount of data being collected to fuel these powerful techniques is monumental, perhaps even alarming. In one analysis, it was estimated that data on the order of zettabytes (ZB) is produced every day [1] – this is certainly hard to imagine.

With all this talk about data, its powers, and its scale, one would be remiss not to consider the source of the data, that is who in the end even makes this whole endeavor possible. The rather simple answer to this question is the individual, the “end user” so to speak. In the interesting dynamic where these new technologies are being created by and for humans, it is ultimately predicated upon the collection of human data, whether it be political views or simply sleep patterns. And to complete this circular dynamic, these massive datasets are then utilized to create tools and technologies that will in turn affect the world around the individual.

To round up this rather brief introduction to data, it is important to note that “data” reaches far beyond was is collected and stored in some database. One may argue that we live in a world where data mining, tracking, monitoring, massive and persistent data storage, and the rapid dissemination of information are all commonplace practices. Data is not simply some tabular information; rather, it is often dynamic, it is quite valuable, and it has become woven into the very fabric of society.

The dangers surrounding the large-scale collection, transportation, and processing of human-originated data has recently brought up concerns regarding the practice as a whole.
1. Introduction

In particular, questions of privacy, security, and even the less well-defined concepts of ethics and morality seem to surround the world of data. Not surprisingly, the implications of such handling of data necessitated the need for legal intervention, in the form of regulations.

Particularly looking at the notion of privacy, one can reasonably posit that the concept is by no means novel. Arguably since the beginning of mankind itself, privacy has inherently been bound with what it means to live as a human. Although it may differ from person to person, we ultimately all desire privacy, in one form or another. This innate desire seems to be endangered when the large-scale collection of data has become not only ubiquitous, but in many cases rather difficult to avoid or control.

In this way, “privacy” regulations, which have existed for decades, have slowly transformed into data privacy regulations, which at their core, strive for the goal of data protection. This presumably occurred as a response to the increasing prevalence of data collection and usage in our society. The overarching mandate of these regulations is the requirement to handle data in a responsible manner, such that the right to privacy of the individual, or “data subject”, is respected. One way of ensuring the compliance to such regulations has been the legal requirement of the necessary “technical measures” that ensure that the above-mentioned rights are preserved. This was undoubtedly performed in order to acknowledge and promote the increasing development of technologies whose sole purpose it is to do exactly this – secure data and protect privacy in a world where data abounds. Thus, the worlds of legal regulation and technological advancement have been undeniably combined, in the manner that they must now work together towards this goal of privacy protection.

The question remains, that in this pursuit for data privacy compliance, or the requirement to comply with privacy regulations, how can the world of technology meet the needs and requirements as legally mandated by an increasing number of privacy regulations? More concretely, the intertwining of two inherently different fields is surely one that does not come without challenges. On one hand, the continual development of promising Privacy-Enhancing Technologies has created hope for the protection of data subjects via technical methods. On the other hand, the existence of regulatory support in the fight for the preservation of privacy can be seen as absolutely necessary. What, however, are the practical challenges preventing the complete harmonization of these two worlds? In what way are certain factors affecting the ability to achieve privacy compliance, even beyond this dynamic? What does privacy compliance even entail, and how does this look in practice?

These are the questions to which this thesis aims to find some answers. In addition, the goal is to begin to work towards some possible solutions that might mitigate the uncovered challenges. This investigation, therefore, is not only to shed light on the process of privacy compliance and identify the challenges in these so-called “technical measures”, but also to explore what might be necessary in order to exact real, tangible change towards a world where privacy is a priority and compliance is a must.
2. Foundations

Before delving into the methodology used to drive this research, it is important to cover some background information that will lie at the foundations of the remainder of the thesis. This background includes both the technological and legal foundations underpinning the notion of data privacy compliance. As such, they must be first introduced.

2.1. Privacy

The notion of privacy must certainly be introduced, as it lies at the core of this research specifically with privacy compliance, and it ultimately has pervaded our modern society as we know it. With this said, the complexity, and perhaps irony, comes with the fact that this term *privacy* is rather hard to define precisely, even with the widespread attention placed on it. This difficulty does not necessarily mean that privacy itself is impossible to understand or grasp; quite on the contrary, it was already mentioned in the Introduction that one can argue for the inherent nature of privacy within humans. It is something that we can, by nature, imagine. And we have done so for millennia.

Yet it is the opinion here that the challenges produced by the desire for privacy materialize with the attempt to translate this innate notion to “the real world”, that is incorporating privacy into everyday human practices and institutions. Now the question becomes: how do I quantify privacy? Implement it technically? Code it into law? Indeed, this is where the meaning of privacy becomes fuzzy.

Concurrently, privacy is perceived differently from person to person, both in meaning and scale. This is something that will hopefully be echoed by the insights of several experts working as privacy professionals, discussed later. The fuzzy nature of privacy is only exacerbated when considering the descriptive (neutral) vs. normative definitions. One may take more of a philosophical stance, grounding their beliefs in the fundamental right to “be left alone”. Yet another opinion may rest in the belief that one’s personal life should be kept private from “the state”. And a final viewpoint may defer to modern privacy laws, demanding the need for responsible handling of one’s personal information. To this last point, one may see regulation of privacy geared more towards access on the one hand or perhaps control on the other. In the end, one would be hard-pressed to refute any of these meanings of privacy, yet how can these discrepancies be consolidated?

As the meaning of privacy is not the focal point of this thesis, it is important to tie the concept back to the possibility of challenges existing in the process of privacy compliance. Before this can be done, some foundation on both the technical and legal sides of modern data privacy must be built. Nonetheless, one may already perceive the possibility for challenges in
2. Foundations

A Note on Privacy

When it comes to the discussion about privacy, several terms come into play. Of course, "privacy" is at the root of the debate, and its general concept was introduced above. Closely related to privacy is the term "data protection", which although being self-explanatory, indeed also grounds itself in privacy as well. This is because of the nature of data, which in the end concerns the individual; therefore, data protection inherently relates back to the concept of privacy. With this being said, data protection is distinct from privacy in the way that the former addresses a particular "application" of privacy, while the latter term is far more wide-reaching. Finally, one arrives at the term "data privacy", which can ultimately be seen as the consolidation of both terms, undoubtedly retaining the emphasis on the data, while also stressing the privacy aspect. Due to this unique dynamic and the diversity held by definitions of privacy, one singular definition will not (and arguably cannot) be selected. The focus, however, will remain on the concept of data privacy. For this reason, data privacy, in short privacy, will be primarily used for the purposes of this thesis, although all three terms and their relation should be kept in mind, especially when one term is more appropriately used in a particular situation.

2.1.1. When Privacy is Threatened

The ensuing discussion about privacy regulations and compliance thereto would be a moot point without the presence of some threat to privacy. Unfortunately, this seems to be the case to an ever-growing degree, presumably fueled by the rapidly growing collection of data, and the potential dubious opportunities this creates. While it is true that massive, rich datasets can be utilized for good-willed and beneficial purposes, one must also consider the flip side to be true. Where there is an opportunity to gain information which is potentially valuable, bad actors may come into play.

The most general form of threats to privacy come in the form of breaches. Largely speaking, a privacy breach entails the loss or theft of sensitive or personally identifiable information (PII), by which the privacy of the effected individuals is not preserved. Of course, what constitutes a breach is not set in stone due to the previously discussed multi-dimensionality of privacy itself. Even so, such breaches occur all too commonly nowadays, and they present a clear and present danger in a world teeming with data – much of which is personal in some way. For an informative, and alarming, info-graphic that tracks the history and severity of modern data breaches, [2] is an excellent start.

One must not be under the assumption that privacy is only at risk when these large-scale "incidents" occur in which entries on the order of millions or more are lost at once. As mentioned, the collection and processing of data is happening on a scale that would likely be unfathomable to past generations. Even well-meaning data processors can find themselves handling very sensitive information, that could turn out to be quite compromising if used in
the incorrect way. Furthermore, the necessary transport of data across nations, and continents, raises concerns with how the privacy of the individual’s data can be best protected.

Looking more deeply into the concern over data privacy, a recent study [3] from 2019 revealed that over 80% of Americans feel they have little control over their data. Furthermore, 7 in 10 of the survey participants responded that they believed their data was less secure than 5 years prior. From these two findings alone, in addition to the other insights provided by the study, one can say data privacy is on people’s minds.

It is in this light, with both the threat of privacy breaches as well as the need for responsible handling of human data, that the need for safeguards to protect privacy has become quite concrete. To tackle this issue, researchers and practitioners from the technical and legal realms, among others, have gone to work.

2.2. Privacy-Enhancing Technologies

It is without a doubt that within the technical sphere, the interest both in academia and in industry has recently sharply risen when it comes to privacy-related research. Indeed, if one searches for the number of publications within the past 20 years simply containing the word “privacy”, the results (Figure 2.1) are quite clear.

![Figure 2.1.: Number of publications containing ‘privacy’ in the title, 2000-2020](image)

Surely, not all of these publications may be directly related to a technical pursuit, but the
2. Foundations

Point nevertheless stands: privacy is becoming more and more relevant. As a further result of this increased interest has come the study and development of technologies whose purpose it is to “enhance” the privacy of a given system or method. As such, the term Privacy-Enhancing Technology (PET), has entered the realm as a concept representing the technical approach to the preservation of privacy. More formally, the European Union Agency for Cybersecurity (ENISA) defines these PETs as “the broader range of technologies that are designed for supporting privacy and data protection”, which address “among other the principles of data minimisation, anonymisation and pseudonymisation” [5].

While many different PETs have appeared in the literature, some of the more popular ones include Differential Privacy [6], Homomorphic Encryption [7], and Multi-Party Computation [8]. These different technologies differ in their use cases, and specifically at what point in the process of data handling and computation should privacy-preservation be applied. In the end, the purpose of Privacy-Enhancing Technologies is to maximize privacy, however defined, with the presence of personal data in a system. Ultimately, they protect the individual’s right to privacy.

2.3. Regulation

When one looks at the legal side of privacy, the response has largely come in the form of regulation. In this way, the protection of privacy has gained legal backbone, and it some places, it is even named a fundamental right by law. From this legal structure surrounding privacy, the concept of data privacy compliance comes to light.

2.3.1. Privacy Regulation, A History

It may be easy to conflate the term privacy regulation with data privacy regulation, seeing the former as a shortened form for the later. In reality, the idea of privacy regulations, or laws, long predate data privacy regulations, naturally. In essence, the initial goal of privacy regulations was to define and protect the legal right to privacy held by all individuals. Many would attribute the birth of modern privacy to the article The Right to Privacy [9] written in 1890 by Louis D. Brandeis, a future United States Supreme Court Justice. In the article, Brandeis defines privacy rather simply as “the right to be left alone”, and he calls for consideration “whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual”. It is interesting to note here that Brandeis’s concern was rooted in “instantaneous photographs” being used by the “newspaper enterprise”. One cannot ignore the already present connection between technology and questions over privacy.

A next major step towards the dawn of modern privacy regulation came with the United Nation’s Universal Declaration of Human Rights [10], published in 1948. In it, privacy is included as one of the fundamental human rights. Specifically, Article 12 declares that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”. As with Brandeis, the role of law, and particularly
its obligation to protect privacy, is brought to light.

In Germany, the birth of modern data privacy protection came with the passing of the Bundesdatenschutzgesetz, or the Federal Data Protection Act, in 1977. This act was monumental in the way that it acknowledges the right to privacy “in the context of modern data processing”. In this way, the fundamental right to privacy is now linked to the (at that time already prevalent) collection of data on a large-scale basis. In other parts of the world, for example the United States, similar acts arose around the same time period, such as the Privacy Act of 1974. This act followed a similar basis as its German counterpart that would come a few years later, laying the groundwork for the fair collection, use, and transportation of personally identifiable information.

Heading back to Europe, the creation of the European Union eventually brought up the need for a unified data privacy regulation, with many of its member states possessing their own disparate versions, such as Germany. Through this need came into the works a massive effort which would result in arguably the most world-changing data protection act to date.

2.3.2. European General Data Protection Regulation (GDPR)

The General Data Protection Regulation [11], often shortened to GDPR, went into effect on May 25, 2018 after being passed by the European Commission. It is touted as “the toughest privacy and security law in the world”, mainly in the way that its implications reach far beyond the European Union. Rather, it has been seen that the GDPR in effect is relevant to any entity collecting or processing data that originates from within the EU. This, as one can imagine, is indeed far-reaching.

The GDPR is quite unique in the way that it provides legal definitions to many of the involved parties and processes in the world of data. Specifically, three parties are involved:

- Data subject – whose data is being processed
- Data controller – who makes the decision on how data is gathered and handled
- Data processor – who actually performs the processing of the data

Particularly looking at the term processing, GDPR rather generally defines this as any action taken on the data in question, whether it be automatic or manual. In this act of data processing, GDPR mandates that seven data processing principles be upheld (Article 5):

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability
2. Foundations

Although it is true that some of these principles are quite self-explanatory, one may also notice that others represent quite subjective concepts, such as integrity or fairness.

Another important section comes with Article 6, in which is outlined the necessary conditions, or situations, in which the processing of data is permitted by law. A final crucial article to laying the groundwork of the regulation is Chapter 3, which covers eight privacy rights of the data subject, namely the right

1. to be informed
2. of access
3. to rectification
4. to erasure
5. to restrict processing
6. to data portability
7. to object
8. in relation to automated decision making and profiling

The defined meanings of each of these can be found in Chapter 3, specifically Articles 12-23.

Privacy Compliance

One of the most interesting aspects of GDPR, and arguably one that makes it so relevant, comes with (data) privacy compliance, the focal point of this thesis. It is arguably most important to begin with the fact that compliance is not intrinsically a target goal of the regulation itself, but it is rather a necessary process born from the requirements laid out by the regulation. Nevertheless, a quick observation of the GDPR text will reveal the word ‘compliance’ used 64 times, as opposed to the obscure term of ‘privacy’, which appears only twice (in the footnotes).

Again, one must remember here the distinction between privacy and data protection. In the words of GDPR, the regulation necessitates a “compliance to the legal obligation” put forward. Putting this into context, it is the obligation of the controllers and processors to ensure and demonstrate compliance. On the other side of this dynamic comes the regulatory authorities, whose purpose it is to monitor the compliance of the aforementioned parties.

Of course, compliance to legal regulation is nothing new. The novelty introduced by GDPR comes firstly with the widespread applicability and enforceability resulting from its nature as a EU-wide regulation. Even beyond this, the implications of the legal obligation to compliance now extended far beyond the EU borders, effectively governing any data processing occurring in, out, or through the European Union. And all of this concerns the protection of data privacy in an age of increasing data utilization – this certainly amounted to quite the change.

Even so, the true power of the GDPR with respect to the compliance process came with its enforcement, or rather the threat of fines to those entities failing to comply. As laid out in Article 83, offenses of non-compliance are subject to fines of 10,000,000 (10 million) EUR or 2% of the entity’s annual turnover, whichever is higher. For more serious offenses, this escalates to 20,000,000 EUR or 4%. The weight of such fines must be considered in comparison to the
threat of fines posed by previous regulations before the passing of this sweeping legislation. As it turns out, previous regulations paled in comparison to GDPR when it came to the maximum penalties. Even the German Bundesdatenschutzgesetz, which represented one of the turning points in the history of data protection regulations, holds a maximum fine of 50,000 EUR, a mere 0.5% of the lower fine in the GDPR. Indeed, quite the difference.

As such, the GDPR introduced a new urgency to the demonstration of privacy compliance, with the possibility of rather crushing fines facing every relevant data processing entity in the event of non-compliance. As they say, money talks. Drawing this back to the purposes of this thesis, the desire (and mandate) for the necessary technical measures to ensure privacy compliance now became a reality, rather than an option to avoid possible menial fines. With such a new and rapid change, the implementation of technical measures for data privacy compliance could hardly come without its challenges (and benefits). Exploring these challenges is a main goal of this thesis.

2.3.3. Others

It is important to note that while GDPR may be the seminal example (at least in the modern day) in terms of data protection regulations, it is by no means the only one. Particularly in recent years, the number of such regulations around the globe has increased, emphasizing the rising global attention to issues such as privacy and data protection. Figure 2.2 shows the relative prevalence of such laws around the world today.

What remains, though, is the need for privacy compliance programs in order to meet the obligations set by any such regulations. In an interesting and possibly foreseeable way, many of the newest regulations certainly take inspiration from the structure put forth by the GDPR, further pointing to the monumental impact of this single regulation (covered in Chapter 10). And now with all this regulation in place, compliance might just become all the more difficult.

2.4. Important Definitions

Here, two important definitions are provided, both of which are terms contained in the title of this thesis. It is seen as crucial to define these terms before proceeding further, as they comprise the overarching basis behind the investigative research performed for the purposes of this work.

2.4.1. "Practical"

The choice of the word “practical” was done with good reason. As the process of privacy compliance, including the demonstration thereof, is something occurring predominantly in practice, i.e. in industry, this is where the investigation into challenges will take place. As will be discussed in Chapter 4, the proxies for “industry” will be the privacy professionals taking part in the interviews, as well as the subsequent survey. As the true practitioners of privacy compliance, it is thought that these people will serve as the best source for the identification
of potential challenges in their daily work. Therefore, “practical” simply means found or occurring in practice.

2.4.2. "Challenges"

While the word “challenges” itself may be self-explanatory, its utilization in the scope of this thesis should also be made clear. The identified challenges should be viewed as hindrances (a word appearing in some of the interviews), or inefficiencies (a word proposed by the author here). Although not completely out of place, the author is hesitant to conflate these challenges with problems or issues existing in data privacy compliance. The true benefit of this distinction is to illustrate these challenges not as inherent failures in the process, but instead as things which can be mitigated or optimized (see Research Question 3 in Chapter 4). In this light, the identified challenges can be viewed in a positive manner as areas where the collective privacy professional community can strive to improve.

2.4.3. "Technical Measures"

The notion of technical measures is something that will be covered more in-depth in the next chapter, yet its initial introduction is fitting here. In short, “technical measures” is used to represent the class of actions that can be taken, with the help of certain technologies, to safeguard and preserve data privacy in some manner. This is often done in order to demonstrate compliance, as required by regulation. Indeed, the motivation for using this term originates from the GDPR text (also covered next), and it was seen as the best, most succinct term to express the use of technology in the pursuit of privacy.
3. Related Work

In this chapter, some related work, or more specifically fields of related work, are introduced in order to provide some further foundation for the scope of this thesis. While it is true that some of these fields do not directly align with the end goal of this particular research, they are all undoubtedly related. As a further motivation, some of the questions raised by these works will actually serve as the basis for the questions asked here. As such, these related works present a sound, yet by no means exhaustive, list for a better understanding of the holistic picture surrounding privacy, compliance, regulations, and of course, technical measures.

3.1. The Technical-Legal Gap

An interesting field of study comes with the investigation into the interaction between the technical and legal sectors, with regards to any pursuit in which these two parties must collaborate. Naturally, one can imagine how this interaction could be a point of interest, in which two fundamentally different fields collide. This is undoubtedly the case in many forms of legal compliance, but especially the case with data privacy compliance. As will soon become clear, this interaction not only occurs, but it is also vital to demonstrating compliance due to the requirement for technical measures for data protection. This requirement, therefore, necessitates the coming together of technical and legal experts to work towards solving a legal requirement with technical tools.

The study of this unique interaction has evolved in two ways. A first way has been the bolstering the use of technology on the legal side, and improving the legal knowledge on the technical side. Specifically with the former, the concept of LegalTech has become quite popular and the source of much research. For an introduction into how this field is emerging and changing the legal sector, the authors in [13] provide a great starting point. The flip side of studying how legal knowledge is disseminated to technically-minded industry workers is a much less-studied topic, and it is certainly one that calls for more attention. Furthermore, in the light of this thesis, this specific question is of great interest.

Another way of looking at the interaction between the technical and legal sectors, particularly with compliance, is through the lens of the “gap” that exists in between. Of course, with such inherent differences, the interaction between both fields might not always be perfect. Indeed, studies have been performed looking into how well the legal community has kept up with rapidly emerging technologies, such as in [14]. Particularly with this study, published already over 10 years ago, the author of this work already saw a growing gap between developing technologies and the ability for the legal side to comprehend and in turn regulate them. Perhaps the best general overview looking at the challenge of “bridging the gap” comes
3. Related Work

with [15], in which the differing viewpoints on privacy from the two fields are studied. Such a challenge can of course trickle down to the individual interactions between professionals in both fields, and it is possibly the case that at this level, challenges can occur. The investigation into this potential “gap” is also of interest in this thesis research.

3.2. Technical Measures

The idea of “technical measures” are clearly central to the work of this thesis, yet it is nevertheless a bit unclear what exactly might be meant by this. Surely, the term is quite unambiguous in the sense that technical measures call for ways in which technology can be utilized for the purposes of data protection, in this case. Beyond that, though, technical measures can take many forms, and some of these are introduced here as preparation for later aspects of this work.

3.2.1. Guidelines

There has been work, mostly on the level of national supervisory authorities, to attempt to clear up the technical side of privacy compliance via the release of overarching “guidelines”. Such guidelines could certainly be useful for the demonstration of compliance, especially when this practice is still quite young, in the newest sense. In Germany, the Standard Data Protection Model (SDM) [16] leads the way. The stated goal of the SDM is to:

"[set] the stage on which legal requirements and the selection and implementation of technical and organisational data protection measures systematically interrelate. Thereby, on the one hand, allowing Data Protection Authorities to conduct more transparent and upright reviews of technical and organisational data protection measures. On the other hand, the SDM provides a methodology for assessing the efficacy of data protection measures required by data protection regulations."

This without a doubt is a great first step towards privacy compliance. More importantly, and something that may lie at the core of some challenges to be explored in this thesis, the text of the SDM acknowledges that:

"Legislation cannot be readily operationalised in a technical manner. Lawyers and computer scientists must therefore find a common language to ensure that the legal requirements are actually implemented technically."

Such thinking relates back to the previous section on the technical-legal interaction, and it is a theme that will undoubtedly arise again.

The Information Commissioner’s Office, the independent data protection authority of the UK, is also regarded to be on the forefront of serving the public interest for all matters data protection. They, too, have released useful guidelines concerning privacy compliance.

Finally, one of the more highly regarded and cited Data Protection Authorities is the CNIL in France. Their many publications include several guidelines pertinent to privacy compliance,
3. Related Work

and particularly technical measures. Some of these include guidelines on anonymization [17] and the security of personal data [18].

While these guidelines are a step in the positive direction, a quick reading of them reveal that technical measures in general are not covered in a thorough manner. Rather, the way in which technical measures may relate to the principles put forth by regulation is the focal point. Exploring the function of these guidelines and where some remaining deficiencies may lie is a goal of this work.

3.2.2. PETs

Already introduced in Chapter 2, Privacy-Enhancing Technologies represent the response of the technical community to the task of privacy preservation in data processing. It is in this way that PETs can arguably be called the “purest” technical measures for data privacy, since this is precisely their purpose. As such, it may be interesting to the reader to learn about the foundations of some of these technologies, if not already familiar. A few of particular interest to the writer are briefly introduced below, but a more comprehensive list can be found on the PETs Wiki page [19].

Differential Privacy

Possibly one of the more interesting cases, and one that has attracted relatively significant attention in the field, is the concept of Differential Privacy. Introduced in 2006 by Cynthia Dwork, Differential Privacy signaled a monumental step forward in the pursuit of “defining” privacy in a mathematical way. The original paper [6] is easily considered a seminal work on the topic. Essentially, Differential Privacy offers a mathematically grounded definition of privacy for individuals in a dataset, with the added ability to “adjust” the privacy parameter, in addition to other benefits. Recent interest in its application to Machine Learning [20] and Deep Learning [21] has spiked, and overviews on the respective topics are included. Differential Privacy’s application to Natural Language Processing, although a budding field, also presents an exciting and worthwhile avenue for future research.
3. Related Work

Homomorphic Encryption

As a Privacy-Enhancing Technology rooting itself in a field that is by no means novel, this PET builds upon more traditional encryption in the way that it allows parties to perform computations on encrypted data, thus protecting the privacy of the individuals therein. The history of such computation and its applicability is covered in [7]. It is particularly interesting to mention this PET, as the concept of encryption as a technical measure is mentioned explicitly a few times in the text of GDPR. Interestingly, in this regulation where almost no mention of specific technologies is made, encryption (as well as “pseudonymisation”) comprise the list of the ones that do. In this way, it may seem that Homomorphic Encryption is particularly relevant to the topic at hand. Either way, this intrinsic vagueness in GDPR is a primary motivator of this thesis, calling into question the applicability, or rather appropriateness, of things such as Privacy-Enhancing Technologies.

3.2.3. Security

The topic of (data) privacy is very closely intertwined with that of security, and as it turns out, the two are many times considered inseparable. Indeed, one could argue that privacy is quite hard to achieve without proper security. Because of this, the attention that has been paid to defining and refining best security practices is important to data privacy, which is clearly the less mature field. In this vein, the progress that has been achieved in the field of security could no doubt bolster some of the open questions concerning privacy. The ultimate question remains: just how much is security related to privacy, if at all?

On the note of national security agencies, the field of security also seems to have the jump in comparison to privacy. Taking the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) [22] as an example, much effort is performed on their side to release official documentation on certain security technologies, guidelines on crisis management, etc. Among these are included minimum standards, which could be closely related to the analogous “minimum technical measures” as required by privacy regulation. Either way, entities such as the BSI serve as good exemplars for the needed progress within the field of privacy. If and to what extent this is the case will also serve as a point of emphasis for the work in this thesis.

3.3. Understanding Data Privacy, Compliance, and GDPR

While the concept of privacy may seem somewhat enigmatic, it is certainly not the case that it has passively been left as this sort of “black box” that is tacitly accepted within society. Rather, there are actually many organizations at work with the purpose of clarifying privacy, corresponding regulations, and anything in between. This work can be seen as necessary, as well as important to increasing the transparency and general awareness of such a vital topic, particularly in modern times. Some organizations and projects of particular interest who are performing (or have performed) quite meaningful work are briefly mentioned here.
3. Related Work

3.3.1. Past and Present Projects

MIREL

The Mining and Reasoning with Legal Texts (MIREL) project [23] began in 2020 with the goal of creating a better framework for working with legal texts. Specifically,

"the MIREL project will create an international and inter-sectorial network to define a formal framework and to develop tools for Mining and Reasoning with Legal texts, with the aim of translating these legal texts into formal representations that can be used for querying norms, compliance checking, and decision support."

This is aimed to be done by combining experts on formal logic, Natural Language Processing, and of course, legal ontologies. This kind of interdisciplinary work is something that will bring up and discussed later in this thesis.

SPECIAL

The Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance (SPECIAL) project [24] ran from 2017 to 2019, with the stated purpose of addressing the contradiction between Big Data innovation and data protection compliance requirements by proposing a technical solution that makes the achievement of both of these goals realistic.

As with the MIREL project, SPECIAL once again based its motivation in a clear acknowledgment of a gap between the technical and legal sides of data privacy compliance. More importantly, it also started vital work towards the creation of a usable framework for compliance (also something directly relating to the challenges brought up later).

DEFeND EU

The Data Governance Framework for Supporting GDPR (DEFeND) project created an international partnership between academia, law firms, and industry to develop “a platform to empower organisations in different sectors to assess and comply to the European Union’s General Data Protection Regulation”. Focusing on GDPR, the project not only emphasized the compliance aspect, but also the process of comprehending and formalizing the GDPR itself, such as aspects of individual rights and consent. As with the other projects, DEFeND also placed emphasis on the technical aspect of compliance, with privacy by design, privacy engineering, and anonymization as central objectives.

3.3.2. Organizations

Harvard Privacy Tools Project

The Harvard University Privacy Tools Project [25] is an interdisciplinary team of lawyers, computer scientists, and sociologists, all of whom are privacy experts. The group explores
privacy-related definitions in law, specifically “the nature of these definitions, the relationships and gaps between them, and potential methods of bridging the disciplinary divide”. Recently, much of their published work has been focused on Differential Privacy. As with other examples, the value of an interdisciplinary team is clearly demonstrated.

Georgetown Law Institute for Technology Law & Policy

Hailing from more of the legal side, the Georgetown Law Institute for Technology Law & Policy [26] is focused on “is training the next generation of lawyers and lawmakers with deep expertise in technology law and policy”. Naturally, this often concerns topics of privacy. The work of this group highlights an important need that was previously introduced and that will become an important theme of this thesis, and that is the (important) role of technical knowledge for people with legal backgrounds.

IAPP

The final group that is indeed of particular relevance to this work stems not from academia, but it is rather an international organization serving as the “comprehensive global information privacy community and resource”. The International Association of Privacy Professionals (IAPP) [27] has emerged as the leading resource for privacy professionals, in terms of networking, resources, and perhaps most prominently, certification. Particularly with their certification offerings, the goal is to certify privacy professionals around the globe, whether they are of law, technology, or otherwise relevant background. In this way, these certifications have largely become the “gold standard” in the field of data privacy, or information privacy as the IAPP often refers to it as. The theme of such an organization as well as the role of certification will certainly arise again later in the findings of this research.

3.4. Privacy by Design

The idea of Privacy by Design, sometimes Privacy by Default or Privacy First, is one that relates directly to the technical measures that are being investigated in this work. Essentially, Privacy by Design promotes that matters concerning the protection of privacy should be integrated into the design process itself, i.e. of any system, rather than being a concern after the fact. This is fundamental in the way that it demands privacy to be considered by default, rather than only by situation or when commanded to do so by law. Of course, this is far easier said than done, and the shift towards this mindset is quite monumental. Cavoukian’s foundational work [28] can be viewed as the pioneer of such thinking, yet its origins may be traced back to [29]. Its influence, nevertheless, has very much influenced modern thought on privacy engineering, producing works such as [30].

The concept of Privacy by Design has been championed by lawmakers and regulators alike, who have in turn designed modern privacy regulations with such thinking in mind. Again, the idea of privacy as the default mode can be somewhat conveniently written into law, but putting it into practice is quite another thing. Articles such as [31] bring to light the inherent
3. Related Work

challenges of privacy first thinking. Further investigating these challenges is a primary goal of this research.

3.5. Data Privacy and Society

At this point, it is hopefully already apparent that data privacy is of paramount importance to individuals, but also to society at large. Surely, the regulations in place to protect this privacy, as well as the technical measures required to comply with them, lie on the surface of how society is impacted by such a pervasive topic. Under the hood, though, privacy reaches beyond technology and policy, existing within the fabric of society itself. This is quite a profound concept, extending beyond the “default” idea that privacy solely involves the individual, i.e. the rights and claims of this single person. Exploring this idea that privacy also has a place in society has been the work of many great researchers, a few of which are mentioned here.

As a starting point, there has been work on analyzing the dynamic role of data and information privacy, tracking its development over time. The authors in [32] do exactly this; furthermore, they look at the concept of privacy, how it relates to other aspects of society, and how the context in these relationships is important. Works like these show the wide-reaching nature of privacy, illustrating that it is something that cannot (and perhaps should not) be confined to individual sectors.

On the topic of contextual privacy, one pervading view is that privacy should be viewed in distinct societal contexts. This comes in contrast to viewing privacy protection solely as the control over the dissemination of data. Arguing that privacy is “one of the most urgent issues associated with information technology and digital media”, Helen Nissenbaum champions the contextual view of privacy in her 2009 work, Privacy in Context [33]. Her proposed framework of Contextual Integrity represents a rather differing approach to information privacy, in the way that the societal level becomes central. Viewpoints like Nissenbaum’s emphasize the societal aspect of privacy, demonstrating the need to focus on the flow of information to preserve the “integrity of social life”.

Another interesting study on the developing concept of privacy in society comes with the juxtaposition of normative and technical concepts of privacy. Concretely, this involves the dynamic between our intrinsic understanding of privacy and what is defined and modeled in technology. This involves the debate over how privacy as a positive, morally justified benefit to humans comes into play when the technical sphere is introduced. In Chapter 2, it was explained how modern privacy regulations demand the use of technology for data protection. The question then becomes: how well do these technologies actually model privacy? In [34], the authors claim a growing divergence in the normative and technical understandings of privacy. Clearly, this could play a significant role in arising challenges in the implementation of technical measures for data privacy compliance.
4. Methodology

This chapter will outline the overarching methodology that will be followed to achieve the goal of this thesis. To make the goals more clear, three research questions are firstly defined. Following this, the two-pronged research approach will be explained, namely the qualitative and quantitative aspects.

4.1. Research Questions

To frame the scope of this thesis, and to better define the end goals, three research questions have been defined as such:

1. How is privacy compliance structured in organizations, from the legal and technical perspective?
2. What are the practical challenges organizations encounter in their privacy compliance programs?
3. How can the identified challenges be mitigated to improve privacy compliance strategies?

The first question is quite straightforward. The goal here is to begin an investigation into the challenges with privacy compliance by first trying to understand how this “process” of privacy compliance is structured within organizations. Surprisingly, there is a rather lack of this research in terms of generalizing the structure of privacy compliance as it appears today, particularly post-GDPR. In this way, this research question will not only pave the way for the following two, but in of itself will also present some new, and in the author’s opinion much needed, findings.

The work posed by the second research question lies at the heart of what this thesis strives to accomplish. It may be useful to first define privacy compliance programs: often this is the name given to the process, or strategy, put into effect by organizations in order to implement and demonstrate privacy compliance. With this in mind, it is the goal of this thesis research to dive into these processes and identify what challenges exist, particularly with respect to technical measures. Beyond this, these challenges will be organized, evaluated, and analyzed.

Finally, the third question presents an interesting case. It is clearly within the author’s knowledge that some of the challenges to be identified are quite large in scope, or even deep-seated. As a result, these identified challenges cannot, and should not, be solved overnight, let alone by the work of a single thesis. The goal with this research question is nevertheless to start the discussion. Performing a thoughtful and thorough analysis on
the identified challenges will certainly point to certain weak points in the field of privacy compliance, and from these, avenues for future work can be identified. Important to note here is that the findings from both this and the previous research questions will be bolstered by both qualitative and quantitative analysis, discussed next.

4. Methodology

4.2. Methodology Design

The methodology of this research follows a two-sided, mixed method approach, as promoted in [35]. Concretely, this method consists of a qualitative study and analysis, followed by a quantitative study and analysis. Also covered extensively in [36], the mixed method approach is crucial in the way that there exists no initial hypothesis in this case, but rather an “inductive theoretical drive”. In other words, the challenges to privacy compliance surely existed, yet these exact challenges cannot be itemized a priori. In addition, the order of these mixed methods is a design choice, and in the context of this work, a sequential model was chosen: qualitative followed by quantitative. The reasoning behind this and a more thorough outline of each method is covered in the following.

4.2.1. Qualitative Study: The Interview

The qualitative study consists of semi-structured interviews, drawing from participants working with privacy in either the legal or technical sectors, or ideally ones that traverse both fields. The interview participants are presented beforehand with a pre-defined set of questions, with the goal being learning about the participant’s role, identified challenges, and future goals regarding privacy compliance within their organization and/or field. From these insights, the main challenge and goal of the thesis is to synthesize the knowledge in order to gain a holistic view of the state of privacy compliance. These insights, in turn, will give way to potential future avenues regarding the bridging of possible gaps in the understanding and implementation of privacy compliance.

The core of this method, therefore, is the interview, and these are crucial to achieving meaningful results in the end. Necessary preparatory work concerning the interviews include discovery and research into potential contacts, collection of background information, outreach, and scheduling.

The most important part, however, lies in the preparation of the interview guide. As such, the questionnaire will be tailored to maximize insights and answerability. This pre-defined set of questions will be forwarded to the interviewee prior to the scheduled interview. As mentioned, the interview takes the form of a semi-structured interview, meaning that it follows a preset script, yet still allows, and often necessitates, some improvisation during the course of the interview. More specifically, the interviews will take inspiration from the framework of appreciative interviews, whose goal it is to generate rich interview data by drawing upon the experiences, opinions, and stories of the interviewee. Such an interview model takes inspiration from appreciative inquiry, originally introduced as a way to promote organizational change [37]. Furthermore, this is done with the mindset of working towards
4. Methodology

Some end goal or improvement. In the scope of this thesis, this type of interview is compatible in the way that interviewees can help work towards identifying the practical challenges existing within privacy compliance by recollecting their own experiences regarding this matter. In addition, this kind of retrospection will be done in an affirmative frame, so as to optimize the generative capacity of the interviews, and ultimately, to provide the richest data in the search for a solution to some of these challenges. With this type of interview, therefore, it becomes important to focus on the tone of the questionnaires, as well as the manner in which the interview is conducted.

Another important aspect of the series of interviews is the ability to adapt the questions as new insights are learned, once again drawing from research methodology proposed in [36]. It is necessary to distinguish between changing the nature of the questionnaire, which would certainly prove adverse to general analysis, and modifying of (sub-)questions, which can enrich future interview findings.

The interview itself will be recorded and later transcribed. Following this, the process of analysis will begin. To aid in this process, the following steps are defined, which follows the steps outlined by Braun and Clarke in their Thematic Content Analysis [38]:

1. Transcript reading – to become familiar with the conducted interview
2. Transcript annotation – to mark important words, phrases, points, etc.
3. Data conceptualization – the creation of categories (themes/codes) based upon the transcript data
4. Data segmentation – the marking of the transcripts according to category
5. Verification – to validate if the themes accurately depict the transcript data
6. Analysis and Results – writing a summary of the interview with the help of the annotated transcripts and its themes (i.e. via this thesis)

In addition to this process, the MAXQDA tool [39] will be utilized to supplement the qualitative analysis of the interviews. Results will be cross-referenced for verification.

Interview Questionnaires

As already introduced, the interviewees consist of professionals, all of whom are involved with the process of privacy compliance in some way. More specifically, these industry experts are selected from both the technical and legal sectors. Because the day-to-day responsibilities are quite different depending in which field the interviewee is active, it was decided that the interview questions be adapted to accommodate these inherent differences. As a result, two questionnaires were created, one for the technical side and one for the legal. While many of the questions are identical or very similar, the unique questions for each questionnaire make it possible to investigate specific aspects of privacy compliance as it pertains to a particular sector. Both questionnaires can be found in Appendix A.
4. Methodology

4.2.2. Quantitative Study: The Survey

The second phase of the core research component of this thesis will be carried out as a quantitative study, supported by the administration of surveys. These surveys will necessarily follow the conclusion of the interview stage, as the results and findings from the latter will be used to formulate the former. In particular, the surveys aim to evaluate the scope and prevalence of the identified challenges from the interviews. Because of this, the Thematic Content Analysis performed on the interview transcripts serves as an important bridge from the qualitative to the quantitative study.

In terms of participants for the survey, the same target audience will be sought after, i.e. privacy professionals, both legally- and technically-oriented. The reasoning behind this format is two-fold. Firstly, the drawing from the same “pool” of privacy professionals allows for the necessary ability to verify the findings from the subset selected for interviews. And related to this, the second reason lies in the fact that surveys are inherently more accessible, requiring far less of a time commitment and not necessitating a certain level of exposure or language capability. As such, it is expected (and required) for the survey participation to exceed that of the interviews.

The survey questions will mainly consist of statements relating to the challenges identified from the interviews. A participant will then have the opportunity to respond to each of these statements with one of five “agreement” responses, taken from the Likert Scale [40]. Specifically in this case, the \{strongly agree, agree, neither agree nor disagree, disagree, strongly disagree\} scale is used. The deployment of this format is useful in the way that it allows for simple, yet meaningful aggregation at the end, which in turn gives way to the relative accuracy and prevalence of the corresponding statements. For example, if a particular statement returns an overwhelming amount of strongly disagree responses, one can conclude that this was a rather rare or unpopular opinion of a particular interviewee, which in reality is not reflected by the privacy community at large.

Although the large majority of the survey questions will consist of these Likert-type responses to perceived challenges, the survey will also contain questions serving two other purposes. The first is accomplished via general background questions, or also questions that reference privacy compliance roles and interactions (the latter does overlap partially with challenges). These types of questions will not only be important to representing the makeup of the participant pool, but they will also help to support the findings for Research Question 1 (the structure of privacy compliance programs).

The second purpose, which comprises the last section of the survey, will probe the participant for their opinion on certain solution concepts introduced in the interviews. Specifically, these concepts will be presented in the frame of their possible ability to mitigate the practical challenges identified through the “challenge questions”. Thus, they will be asked to verify whether they believe these concepts would be effective and/or worthwhile. In addition, this section contains a space allowing for free input from the participant, in order to further bolster the findings for Research Question 3 (how to mitigate the identified challenges).
4. Methodology

Survey Questions

The full array of survey questions, and a link to the (closed) survey itself, are provided in Appendix A. Unlike for the interview questionnaires, however, it is not recommended for the reader to look over the survey questions at this particular point. The main reason for this lies in the two-pronged nature of the research component that has been outlined in this chapter. Only through the analysis of the interview findings could the survey and its questions take form. Therefore, it would make the most sense first to delve into the interview results, covered in the next chapters. Once the challenges are introduced and explained, a mapping from these to the survey questions (a one-to-many mapping) will be presented. From here, the survey questions will have a formal basis in the identified challenges, and only then will they become the most clear. On this note, the interview makeup and findings are now discussed.
5. The Interview Makeup

In this chapter, the makeup of the interview process is described and analyzed, in preparation for the analysis of the actual interview findings themselves. This initial step is important in a two-fold manner: (1) to outlining the process followed for procuring participants and carrying out the interviews, and (2) to understanding and visualizing the demographics of the interview participants. The ultimate goal in these proceedings was to obtain a representative sample of privacy professionals, and accordingly, to conduct a tailored, yet generalizable interview experience.

5.1. Identifying Participants

The privacy professional field is a large and ever-growing group of people, particularly in light of the aforementioned “boom” created by the GDPR. As such, the pool of possible participants represented a bountiful, yet daunting, number of potential contacts for the interview. To simplify the process of identifying interview participants, the source of contacts was limited to four avenues:

- **Personal contacts**: people whom could be immediately contacted as a result of a shared connection
- **Pre-saved contacts**: i.e. from the work of previous research, in which contact lists were created.
- **Top search results**: i.e. via LinkedIn, where terms such as ‘privacy professional’, ‘privacy engineer’, ‘data protection officer’, or ‘data privacy lawyer’ were entered.
- **Referrals**: once initial interviews were conducted, people referred to within these could then be contacted, now with a shared point of reference.

Once these contacts were identified, several steps were followed to initiate contact, present the opportunity for an interview, and (hopefully) schedule the interview. This process is briefly outlined below:

1. Informally ask for an interview via direct message (only if found on LinkedIn).
2. Follow-up with / send a formal email invitation, outlining the purpose of the research and structure of the interview.
3. Schedule interview.
4. Before the actual interview, provide the set of questions so that the interviewee can prepare his/her responses.
5. The Interview Makeup

Particularly with the last point, this step was seen as necessary due to the nature of the semi-structured interviews. Since the interviewee was provided with the questions beforehand, the general flow of the interview would be known in advance, allowing for impromptu follow-up questions and deeper discussions.

Looking specifically at the contacting process, it was well within reason that the number of scheduled interviews would be far less than the number of contacted potential interviewees. To visualize this gap, the following graph displays the relationship, broken down into technical and legal contacts:

![Visualizing the Contact Process](image)

Figure 5.1.: Visualizing the Contact Process

‘Contacted’ denotes the people to whom a formal invitation for an interview was sent, but from whom no response was received. ‘Reject’ in turn denotes a received response turning down the opportunity. Finally, 'Interview Complete' is self-explanatory: the full contact process was completed, and an interview was successfully conducted.

From Figure 5.1, one can see a fairly even balance of technical and legal interviews conducted, with 7 and 8 respectively. In contrast, a quite clear imbalance of potential interviewees contacted is highlighted. This discrepancy can be partially attributed to the fact that more contacts falling into the “Personal Contacts” category were on the technical side – a more in-depth breakdown of this follows next. In the end, one can calculate a response rate (defined as the percentage of successfully scheduled and conducted interview) of 28.5%. Note that this only includes people with whom at least Step 2 (see above) of the contacting process was reached, i.e. not included are unanswered LinkedIn messages.

In this vein, it is interesting to dive deeper into these numbers, breaking them down into each of the four defined categories of contacts introduced above. The ensuing graph in Figure 5.2 simplifies Figure 5.1 into two results categories, either ‘Interview Complete’ or ‘No Interview’ (‘Reject’ + ‘Contacted’).
5. The Interview Makeup

Figure 5.2.: Contacts, broken down by category

A quick analysis of Figure 5.2 shows first and foremost that the utilization of pre-saved contact lists is not helpful. This most likely can be attributed to the fact that while such lists might be useful for certain purposes, the contacts therein are not guaranteed to be of exact relevance to the project at hand, i.e. this research. Among the most fruitful of the contact categories are those from the “Top Search Results”. This is quite surprising, but upon further thinking, it could be logical that these contacts would be the ones most willing to participate in an interview; indeed, these interviews counted amongst the most insightful ones, as will be alluded to in the subsequent chapters. Finally, in both top-level categories, personal contacts and referrals also played a significant role, emphasizing the value of personal connections with matters such as face-to-face (hour-long) interviews.

5.2. Interviewee Demographics

The purpose of this section is to provide the reader with a broad overview of the makeup of the interviewee pool. Accordingly, the chief goal is to convince the reader of a reasonably diverse and representative sampling, while also providing visual information of possible interest. This information is of course kept anonymous and as general as possible while still remaining meaningful.

5.2.1. Experience

One of the first interview questions asks the participant how many years of experience he or she has. Particularly of interest here is how many years of experience in the privacy field are
5. The Interview Makeup

This specific “statistic” is interesting as it will play a significant role into following the development of the field of privacy compliance, especially in light of impactful events such as the passing of the GDPR. Also keeping in mind this number when analyzing the statements of particular individuals, it is without a doubt plausible that years of experience will influence (shape) their opinions and viewpoints. More on this in the forthcoming chapters, but for now, Figure 5.3 illustrates the distribution of years of experience among the interviewees, separated in buckets.

Figure 5.3 shows a relatively clear distribution, namely with the main concentration on the “tail ends”. Of particular noteworthiness is the amount of interviewees who are new (0-3) to the field. The insights from these interviews, when juxtaposed to those of more seasoned privacy professionals, will certainly prove to be valuable.

Another way to visualize the overall experience of the interview pool is through the presentation of the accumulation of experience over the years, which can give light to the relative balance of newer versus more experienced perspectives. This is done in Figure 5.4, which presents this data alongside a few, select “data privacy events”. A clear “exponential” growth is seen, pointing to a non-linear accumulation, i.e. heavy on the back end. In total, the interviewees participating in this research collectively possess approximately 154 years of industry experience.

Specifically to the point, an interesting point of reference to take is the adoption of GDPR, which occurred in April of 2016. The importance and impact of this event (but most notably its implications) will most likely become clear throughout this work. Figure 5.5 compares years of experience before and after this monumental event – a fairly even split was observed.
5. The Interview Makeup

Figure 5.4.: Interviewee Accumulated Years of Experience

Figure 5.5.: Years of Experience, Pre- and Post GDPR Adoption
5.2.2. Gender

One would arguably be remiss not to include an overview of the interviewees themselves, and to this, gender can be a rather simple, yet powerful summary statistic. Figure 5.6 display the overall split in male versus female interviewee participants in this study.

Figure 5.6 shows a significant majority of male participants. Of course, many factors could have come into play during the contact process that could have resulted in such a skew. Nevertheless, breaking down Figure 5.6 by sector (technical or legal) provides some interesting and otherwise hidden insights, illustrated by Figure 5.7 (color coding is preserved).

Without diving too deeply into matters such as the gender gap in certain fields, the picture painted by Figure 5.7 is telling in a couple of ways. A study published by the IAPP [41] claims that a “virtually equal” split between genders exists within the privacy profession. The legal portion of Figure 5.7, under which all participants would count as *privacy professionals*, mimics this essentially equal split. In contrast, another recent study [42] claims that a 28.8% representation of women is held in the tech industry. Although not completely on point, the interview participation from the technical side of privacy compliance somewhat mimics this relationship. The discussion on gender will end here for the scope of this thesis; undoubtedly, the very broad statistics provided here raise some interesting findings and questions.

5.2.3. Location

A final interviewee demographic that will analyzed is location. By location is meant a two-fold observation: (1) location of the interviewee and (2) seat (“headquarters”) of the represented
5. The Interview Makeup

Company or organization. In some cases, these will overlap, in others not. Locations are generalized so as not to be overly specific, yet still provide a reasonable geographic sense. This particular analysis is thought-provoking in the way that particular opinions expressed by be representative of certain cultural, organizational, or otherwise geographically-tied factors. A more in-depth exploration into this notion will be carried out later in this work.

Figure 5.8 describes an interview pool concentrated in the major areas of the United States, Europe, and parts of Asia. As it turns out, these regions are the key parties involved in the current field of privacy (compliance). Additionally, there was a good diversity of participants with respect to the inner-regions within these covered continents. The eastern, mid, and western United States was represented. In Europe, participants stemmed from the UK, central Europe (the majority), as well as the Balkans. Finally in Asia, the key countries of India and China were included. Note that in these sweeping statements, it is not necessarily indicated whether the countries or regions represented trace back to an interviewee or organization. While the diversity and number of countries represented could certainly have been improved, the author holds in belief that the resulting sample is sufficient for at least beginning the discussion on the topics and challenges introduced in this thesis.

5.3. The Interviewees, Summarized

In Table 5.1, the reader will find a codified, anonymized table of the interviewee participants, which includes their relevant information. Some of this information was already presented visually in the above sections. Most importantly going forward, though, is the unique
The Interview Makeup

Figure 5.8.: Location of Interviewees and their Organizations

Interviewee code assigned to each interview participant. These codes will be referenced in the remainder of this work in order to cite specific statements or express a particular opinion held by the corresponding interviewee. Note that codes suffixed with a ‘T’ denote a technical contact, ‘L’ a legal, and ‘LT’ a contact who “has a foot in both doors”. Also note that with the interviewees in this last category, it was always the case that the legal questionnaire was used, as these participants were officially in this profession.

Some other explanatory notes to Table 5.1. For no other reason than logical, the order of the table follows the order of the conducted interviews, which spanned a three-month time period from August to November 2021. The position named in the table is the one provided by the interviewee during the initial part of the interview. The generalized description of each corresponding organization has been created by the author of this thesis, so as to provide meaningful information regarding the relative size, the originating region, and the main purposes of each organization. “Exp.” denotes years of experience, shortened in order to preserve readability of the table. This attribute was discussed previously and depicted in Figure 5.3. Additional information is provided in the cells where a parentheses are included, which indicates cases in which the interviewee has longer relevant experience in the technical or legal fields, and later on began working as a privacy professional. Thus, the number in the parentheses is the number of years worked as a privacy professional. In a similar way, “Dur.” denotes duration of the interview, which will not merit any further analysis in the remainder of this work. It is, however, useful to verify the relative uniform duration across all interviews, with one outlier (I3-L, due to a scheduling conflict).

All in all, the interviews conducted amounted to roughly 15 hours, resulting in 236 pages of cleaned transcripts.

With the makeup of the interviewee pool fully elaborated, it now becomes time to dive into the interview findings themselves.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I1-T</td>
<td>Privacy Engineer</td>
<td>Large American media conglomerate</td>
<td>10+</td>
<td>54</td>
</tr>
<tr>
<td>I2-T</td>
<td>Privacy / Security Architect</td>
<td>Large German multinational software corporation</td>
<td>6</td>
<td>52</td>
</tr>
<tr>
<td>I3-L</td>
<td>Privacy and cybersecurity lawyer</td>
<td>Chicago law firm</td>
<td>20+</td>
<td>32</td>
</tr>
<tr>
<td>I4-T</td>
<td>Privacy Engineer</td>
<td>Large American multinational tech company</td>
<td>5+</td>
<td>70</td>
</tr>
<tr>
<td>I5-LT</td>
<td>DPO, Managing Director</td>
<td>Small Munich-based data protection software company</td>
<td>4</td>
<td>50</td>
</tr>
<tr>
<td>I6-T</td>
<td>Software Architect</td>
<td>Large German multinational tech conglomerate</td>
<td>3</td>
<td>50</td>
</tr>
<tr>
<td>I7-L</td>
<td>Lawyer / external DPO</td>
<td>Small German data privacy company</td>
<td>20+</td>
<td>55</td>
</tr>
<tr>
<td>I8-L</td>
<td>Group Data Protection Counsel</td>
<td>International financial technology corporation</td>
<td>6</td>
<td>60</td>
</tr>
<tr>
<td>I9-T</td>
<td>Privacy Engineer</td>
<td>Large US Tech Corporation</td>
<td>8</td>
<td>65</td>
</tr>
<tr>
<td>I10-LT</td>
<td>Legal Counsel</td>
<td>Global Web Consortium</td>
<td>25</td>
<td>60</td>
</tr>
<tr>
<td>I11-L</td>
<td>Legal Counsel</td>
<td>Munich-based digital privacy consulting firm</td>
<td>3</td>
<td>50</td>
</tr>
<tr>
<td>I12-L</td>
<td>DPO</td>
<td>Munich-based consulting firm</td>
<td>20</td>
<td>55</td>
</tr>
<tr>
<td>I13-T</td>
<td>Security and Privacy Architect</td>
<td>Large German multinational tech conglomerate</td>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>I14-L</td>
<td>Compliance Officer</td>
<td>British-based news corporation</td>
<td>3</td>
<td>50</td>
</tr>
<tr>
<td>I15-T</td>
<td>Privacy Engineer</td>
<td>Chinese multinational tech corporation</td>
<td>15</td>
<td>60</td>
</tr>
<tr>
<td>I16-L</td>
<td>Legal Associate</td>
<td>Indian-based law firm</td>
<td>3</td>
<td>55</td>
</tr>
</tbody>
</table>

Table 5.1.: Coded Interviewee Table
6. The Structure of Privacy Compliance

In this chapter, the process behind privacy compliance is outlined and analyzed, and subsequently compiled into a formalized structure. This structure includes the parties involved, their individual responsibilities, and of course, the interaction that takes place between the entities. These insights are grounded in the findings resulting from the interviews, where a main emphasis was placed on inquiring about the day-to-day duties and interactions of the various privacy professionals interviewed. Thus, the goal of this chapter is not only to answer Research Question 1 as completely as possible, but also to lay the foundation upon which the following two questions, or rather their answers, will be built upon. More specifically, without a sound understanding of the driving mechanisms of privacy compliance today, the challenges within relating to the implementation of technical measures, and their possible solutions, cannot be fully grasped. As a final introductory note, the findings below stem for the most part from the interview findings, so as to stay true to the methodology outlined in Chapter 4. Where necessary though, external resources may be consulted to round out an explanation or discussion. Where direct quotes out of an interview are used, these will be demarcated with the corresponding interviewee code; this is also true for the rest of this work.

6.1. Definitions / Clarifications

A couple of important definitions are provided to avoid ambiguities for the remainder of this chapter (and work).

6.1.1. Organization

In the scope of this work, the term organization is used to indicate a general legal entity comprised of an association of people sharing a common purpose. Other terms often used interchangeably with organization are company, business, or even institution. Although the true distinction between these most likely could be made, this is outside the scope and beyond the knowledge of the author. As such, the terms will also be used interchangeably here, most often with organization.

6.1.2. Talking About Compliance

One initial question in the exploratory research performed became, how does one talk about privacy compliance? This means not the processes within, but rather the term itself. Through some research, a few terms and phrases came up, some of which have already appeared
in the Research Questions of Chapter 4. Although the reference to the process of privacy compliance will most often be made, more specific terms pertaining to privacy compliance within organizations are those such as privacy compliance programs or strategies. Moreover, as already previously introduced, the goal of such practices are for the demonstration of compliance to the appropriate regulations. While the intricacies of such terminology are not overly pressing to the work of this thesis, their introduction may serve as useful in following some of the wording used for the remainder of the work.

6.2. Roles and Responsibilities

In this section, the major roles involved in privacy compliance are introduced. In addition, their main responsibilities are elaborated upon in order to best paint a picture of the privacy compliance structure.

6.2.1. Legal

Legal Counsel

Starting off with the legal side of privacy compliance, the first party involved is quite understandably the legal team. It is important to note straight at the beginning that the term “legal team” and “legal counsel” are quite umbrella terms, and are sometimes used interchangeably. Furthermore, the exact location of the legal team can differ significantly, with larger organizations having “in-house counsel” and an internal legal team (or teams). In the case of smaller organizations or ones where the constant availability of legal support is not necessarily needed, “outside/external counsel” quite often composes the legal team of that particular entity.

With the concept of a legal team is meant a group of practicing lawyers and/or legal associates. Specifically relating to the topic of data privacy compliance, many of these lawyers will be specialized in sub-fields such as privacy, data protection, cybersecurity, and the like. With outside counsel, it is often the case that these firms themselves will be specialized. In these cases, though, a specialization in data privacy does not imply that the firm only handles compliance; this sub-field also includes services such as litigation or breach and incident response.

While the job itself might be quite complex, the stated responsibilities of legal counsel with respect to privacy compliance is rather straightforward. From the technical perspective, “Legal interprets everything… their job is to make sure we’re staying up to date, trying to be compliant.” (I1-T). What this means is clear – legal support is there to provide interpretation of the relevant regulations, so that the other (non-legal) parties can properly carry out and demonstrate compliant systems. The job of outside counsel is virtually identical: “We’re outside counsel, which means that we advise clients on the legal requirements.” (I3-L). Again, this emphasizes the advisory nature of legal support, that is the guidance provided by legal as the interpreters of laws and regulations.
6. The Structure of Privacy Compliance

A final responsibility of the legal teams is distinct from the guidance aspect just discussed. This additional duty was brought up in a technical interview, where the interviewee acknowledged the “teams of lawyers who engage with, like the European Commission, there are teams who side kind of with the nation state, you know, like engaging with Congress.” (I4-T). Here it is displayed that the role of legal extends beyond the in-house counsel / client advisement interactions to more of a role as a liaison. In this way, legal counsel serves an important and dynamic function in the process of privacy compliance.

**External Consultant**

Also under the legal category but strictly distinct from legal counsel is the role of an external consultant. This person is most often involved with smaller to mid-sized organizations. As this role is of the consultory nature, it is inherently external, or a position that must be contracted outside of a particular organization seeking consultation. Crucial to note with this role is that there is no expectation that the consultant is a practicing lawyer. Furthermore, this seems rarely to be the case; of the interviewees serving in this role, none were lawyers.

With regards to the responsibilities of external consultants, the intersection with legal counsel (lawyers) becomes somewhat greater. Simply stated, consultants of this nature are “specialized in providing support on privacy topics” (I7-L), especially including compliance. A more in-depth description of the role describes how consultants “support and consult with companies that want to process data of individuals... to make sure that the client is really handling the data in a legal matter, and in a secure space.” (I11-L). One may already see the possible overlap between the job of the consultant and of legal counsel, essentially both relating back to providing legal backbone to the processes involved with privacy compliance. The concept of the advisement provided by lawyers and the consultation provided by consultants can, rightly so, be conflated. The true distinction comes from the fact that legal advice provided by a practicing lawyer cannot be replaced by that of a consultant, under the eyes of the law.

A final function of both lawyers and consultants will be introduced here and expanded upon later, and that is the role of a Data Protection Officer (DPO). This specific role is explicitly mentioned in the GDPR, and as a result of its passing, has become a necessary and important role in the function of countless organizations. In this way, lawyers and consultants can also serve as DPOs, where they “ handle DPO services, we provide [advisement] and consulting on data protection and privacy... we also train some stakeholders during and after the process.” (I16-L).

**Compliance Officer**

A final “legal” role is one that is arguably the most specific to privacy compliance itself. This is the role of a compliance officer within companies or organizations. The compliance officer role is quite unique in the sense that it is not a strictly legal role, in the way that a lawyer might be. Rather, “It’s a bit more on the legal side of it, without stepping too far into legal because we do have a legal team... we’re simply there for the operational risk, and really
deciding what that risk is meant to look like for us.” (I14-L). This explanation introduces the extremely vital concept of “go-betweens” in the privacy compliance structure, something that becomes very important and that will be expanded upon in the upcoming sections.

As is made clear by the title, the compliance officer essentially is involved with all things compliance within an organization. In the words of one such officer, “A lot of what we do is obviously ensuring that data privacy alone, amongst other compliance areas are [followed] for the rest of business… privacy obviously being the larger one of the pillars.” (I14-L). This highlights that although data privacy is not the singular focus of compliance processes, it has recently become a rather important one. Because of this, compliance officers also serve an integral role in proper compliance. With this, though, it is not clear how widespread this role is, or in how many organizations such a role exists.

6.2.2. Technical

Looking at the specific scope of this thesis work, the technical influence on privacy compliance becomes clear. Taken from another angle, the technical measures required for privacy compliance have certainly impacted the structures existing within the technical verticals in organizations. Some of the most relevant roles are discussed here. Note that while the roles discussed below come from specific interviewees at particular organizations, it is attempted to explain their general relevance to the technical side of privacy compliance. With that being said, it may very well be the case that some of the below-mentioned roles and responsibilities are not applicable to certain other organizations. It is the author’s opinion that these roles should nevertheless be introduced to paint a complete picture of the field as it stands today.

Product Team

Starting off as with legal with more of an umbrella term, the concept of the product team encompasses the team involved the design and implementation of “the product”. In the technical sense, this usually refers to the system(s) being developed for the market. Specifically on the product team may be roles such as (software) developer and engineers, as well as the appropriate leadership roles.

In a discussion about the involvement of the product team in privacy compliance, one interviewee paints an excellent picture of the connection:

When a project is being set up, you usually have project owners, you have the business unit.. the information security officer is identified… in the very initial phase of the project itself, you have to discuss with the Data Protection Officer and Information Security Officer what this project is about, you have to perform a business impact analysis. (I6-T)

This picture introduces several important parties to the privacy compliance structure. The product team, lead by the project owner, is connected with the necessary officers to perform a risk analysis of the proposed project, which then serves as the basis for determining the necessary measures for compliance. The role of the project owner is also emphasized as “the
first point of contact [regarding privacy]... it’s the project owner’s responsibility to deal with communication and bringing people together.” (I6-T). Through this, one can see a hierarchy being built with regards to privacy matters within a technical vertical.

While the discussion of the role of the product team, as well as its distinction from the business unit certainly merits more than a few paragraphs, the main function of its relevance to privacy compliance is introduced here. Ultimately, the purpose of many organizations can be boiled down to the products it develops; in this way, compliance to regulations will always be inextricably tied to the roles within.

Architects

One specific role hailing from the technical vertical is that of the architect. Starting with the more general term of Software Architect, this person is more involved on the design side, rather than development or implementation. For this reason, the architect’s role becomes very important in the implementation of compliant systems, as it is in this stage of (pre-)development that sound privacy-respecting practices are planned and incorporated.

In the words of a Software Architect, “At the architecture level, you need to have a very good understanding of the entire data flow within the structure.” (I6-T). This concept of data flow became an often recurring theme in the interviews, both on the technical and legal sides. As the root of data privacy can be traced to the flow of data, this statement from I6-T can indeed be argued for.

The role of Software Architect is sometimes specialized to Privacy Architect, or also Privacy and Security Architect, or even Enterprise Architect (more generalized) in larger organizations. With this, the emphasis on the design of privacy-preserving, secure systems is made concrete. The Privacy Architect can sit “Directly below the Chief Security Officer, working on regulatory questions, new tooling, and so on.” (I2-T). One sees here that this specific role begins to near the legal side of compliance, while still obviously remaining technical. In summary, the role is “essentially about optimizing business processes” (I2-T) within an organization. Although this description is certainly rather broad, privacy compliance without a doubt fits under this job description. As will be explored later in this work, compliance indeed becomes paramount in the optimization of business processes (and value).

Management

While the roles on the management level are not technical per se, the focus of this thesis on technical measures usually involves technical organizations in some manner, under which the management tends to be technically-oriented. In either sense, the role of management is vital in the privacy compliance structure, something that will be revisited often throughout this work.

The concept of management first and foremost includes the “C-Suite” executives responsible for the leadership and direction of organizations as a whole. It is often the case that “decisions making [regarding compliance] come from a couple levels above” (I1-T), i.e. management. Specifically in the case of I1-T, “it is the head of the engineering vertical that really makes
those decisions.” This begins the discussion on the importance of management-level roles when it comes to privacy compliance.

In regards to specific roles, some have already been introduced. One in particular that came up in multiple interviews is the (Chief) Information Security Officer. Interestingly enough, the title is misleading in the sense that the responsibility for privacy matters also falls under this role as well. More on this distinction/conflation later. Put in rather general terms, “The ISec officer is responsible for ensuring there are no loopholes” (I6-T) in the development of compliant systems. It is also interesting to note here that the discussion of the privacy compliance structure, so far on the technical side, has been confined to the “engineering vertical”, including management.

**A Distinction** While many of the roles discussed already, and those to follow, are “generalized” to form a more encompassing picture of the privacy compliance structure, one distinction has been left separate. Specifically, as will be seen in Figure 6.1, the distinction within the “manager” role between Engineering Manager and Program Manager is left intact. This is done as a result of both roles being brought up in various interviews, but in a way that leads the author to believe that the two roles should not be conflated. Indeed, if one performs some cursory research into this distinction, one may agree with their separation. An engineering manager is focused on “the technological problem-solving ability of engineering and the organizational, administrative, and planning abilities of management in order to oversee the operational performance of complex engineering driven enterprises” [43]. On the other hand, a program manager is “a strategic project-management professional whose job is to help oversee and coordinate the various projects, products, and other strategic initiatives across an organization” [44]. While both can clearly be seen as “vertically-oriented” management roles, the former is seemingly focused on engineering matters, while the latter plays a strategic role in the execution of projects, also introducing a “horizontally-oriented” aspect. Nevertheless, both roles certainly play an important part in the process of privacy compliance, as they provide direction to some of the lead engineering roles involved within the technical side.

**6.2.3. External Stakeholders**

**Third Party Vendors**

In the process of privacy compliance, much of the work when it comes to tooling and automation is often outsourced to third parties. These “vendors” often comprise of external companies providing a service or technology as a “technical measure” for compliance. A prominent example is consent management systems, such as those provided by major players like OneTrust, marketed as the “The #1 Most Widely Used Platform to Operationalize Privacy, Security & Data Governance” [45].

One interviewee confirms that “most of the external interactions we have is with third party software providers for security functions and when it’s about tooling.” (I2-T). This solution is
useful for organizations looking for an “out-of-the-box” system, yet the introduction of third parties into a process centered on privacy can also raise concerns and/or challenges.

Although the role of these third parties is intriguing, they will not be further discussed due to a lack of evidence from the interviews. Truly, though, the case can be made for their inclusion in Figure 6.1.

**Supervisory Authorities**

The role of supervisory and regulatory authorities was introduced in Chapter 3, where their work on providing guidance for technical measures was discussed. These authorities can serve as a useful resource for organizations in guiding privacy compliance programs. It is interesting to note that while several interviewees mentioned this sort of interaction only in passing, a clear need for more interaction was often elaborated upon (see Chapter 9).

**The Customer**

The final external actor, arguably the most important, is the customer. While this stakeholder was not often mentioned explicitly, the implicit inclusion of this person was without a doubt always tacitly understood. One must not forget that in the myriad of discussions surrounding privacy, compliance, technical measures, regulations, and so on, the customer (user, individual) is the ultimate stakeholder, whose data comprises the crux of the issue. Accordingly, one would be remiss not to mention (albeit briefly) this crucial stakeholder.

### 6.2.4. The Go-Betweens

The final category of roles involved is one that merits a rather in-depth discussion. These roles the author has defined as the *Go-Betweens* (also known as the *in-betweens*) of the privacy compliance structure. Such a label has been used to indicate the inherent interdisciplinary responsibilities possessed by these roles, often transcending one single field or sector. As it turns out, two particular parties in the process of privacy compliance have been selected, one stemming from the technical side and one from the legal, but both of which must necessarily cross the technical-legal gap (in as much as this exists) to perform their duties to the fullest. These new and promising, yet challenging and dynamic roles are outlined in the following.

**Data Protection Officer**

The role of the Data Protection Officer (DPO), is a fairly novel concept, rising out of the text of the GDPR. Specifically in Articles 37-39, the designation, position, and tasks of a DPO are covered. The general work of a Data Protection Officer includes aiding in the compliance process for relevant data protection laws, accomplished via “monitoring specific processes, such as data protection impact assessments or the awareness-raising and training of employees for data protection, as well as collaborating with the supervisory authorities.” [46] What is arguably the most interesting part of this dynamic position is the relative freedom allowed to organizations with regards to selection of a DPO. First and foremost, the appointment of
6. The Structure of Privacy Compliance

a DPO is not a blanket requirement, but rather it depends on the data processing activities of the organization in question. Specifically, if “core activities consist of processing sensitive personal data on a large scale or a form of data processing which is particularly far reaching for the rights of the data subjects, the company has to appoint a DPO.” [46] An extra point is made that this appointment does NOT depend on company size. The main flexibility with the selection of this role lies in the choice of an internal or external DPO, where the former can be an employee and the latter can be outside counsel or a consultant, provided these people can provide the necessary expertise.

Beyond what is mandated in the GDPR, the Data Protection Officer role has clearly become central to the privacy compliance process. This illustrates the breadth of this regulation, requiring organizations across the globe to abide by such requirements, and this was certainly reflected in the interviews.

What also shone through in the interviews, and what may not be immediately apparent from the text of the GDPR, is the unique nature of the role itself. The DPOs are “de facto go-betweens” (I3-L), and in the words of an acting DPO, “The person taking care of data protection in an organization needs to be hybrid.” (I5-LT). Indeed, as mentioned before in the outline of the product team, the DPO (team) becomes integral to the onset of any project that involves the handling of data. In larger organizations with a dedicated data protection team, a person from this team must be identified and included in a project before this new project can proceed (I6-T). Apart from the DPO, this team may include one or several lawyers.

Analyzing this “hybrid” role of the Data Protection Officer, it becomes quite clear what is meant here. At the core of the responsibilities of this person lies the task of liaising between what is said in the law, i.e. the letter of the law, and how this is implemented in practice. In the scope of this thesis, the technical measures required for privacy compliance serve as a major factor in this dynamic, and the DPO must navigate these waters. Ultimately, it is crucial to note that, “At the end of the day, the data protection officer is more a legal person than a technical person.” (I2-T). Fortunately, a technical counterpart is emerging in the field today, which offers a promising balance in the necessary role of go-betweens.

Privacy Engineers

The concept of a privacy engineer is without a doubt relatively new, and it is up and coming in the sense that such a role has not been uniformly adopted across the industry. The privacy engineer’s job is extremely interesting in the way that it is somewhat less technical than say, a software developer, despite what the name might imply. Rather, a privacy engineer lies very much in the in-between area. To provide a better sense of the role, the interviewees serving in this role shed some great insights.

Starting off with broad definitions of the role, one privacy engineer views the position as a “go-between between the end consumer product and the legal team. It’s all gonna filter through us.” (I1-T). Specifically the use of the term go-between echoes what was also said from a legal perspective regarding the DPO. Ultimately, this resonance inspired the use of the term itself for this important middle ground. Similarly, another privacy engineer sees the role from this “in-between” perspective: “We sit at the gap between making sure that we
understand what is available information, and what’s our guidance from legal.” (I4-T). A more specific definition comes with “Privacy engineering is really about ensuring there is the trust at the level of technology to protect privacy and to mitigate privacy risks.” (I9-T). Finally (and simply): “I’m really in product design.” (I15-T).

If one analyzes these somewhat varying definitions of privacy engineering, there does indeed exist a common theme. First, to reiterate the idea of the hybrid, in-between nature of the role. As with the DPO, the privacy engineer sits at the intersection of law and technology, but in this case, with a firmer foot in the technology door. Nevertheless, the interaction with legal support is clear, implying the necessity for some degree of legal literacy. Ultimately, this role boils down to the assurance of privacy protection in the design of products (technologies, systems) themselves, giving credence to the short, yet powerful definition from I15-T.

On an organizational level, there does not seem to be a fixed location to position the privacy engineer(s). According to one engineer, you “can either align a privacy team vertically, according to a product or you can align it horizontally.” (I4-T). In the end, this seems to be a decision for management.

Looking deeper into the role, it is interesting to note that “you, more or less, get very different backgrounds in privacy engineering.” (I4-T). Not only does this once again stress the hybrid nature of privacy engineering, but also within this statement (and from the interview context), it was learned that privacy engineers need not necessarily be experts in the finer details of the technologies and implementations themselves. Instead, their expertise in data protection, privacy design principles, and the implications of privacy to society at large are what make the role valuable. Thus, privacy engineering provides an unique supplement to the design and implementation of technology. A somewhat divergent view from that above comes from another privacy engineer: “I’m working on the technology side and really want to promote these technologies more than the compliance.” (I15-T). Such a statement serves as a reminder that the privacy engineer undeniably still resides on the technical side of compliance; furthermore, the juxtaposition of technology and compliance introduces an interesting debate that will be explored later in this work.

A major responsibility of a privacy engineer comes as a policy maker. According to I4-T, a main task of a privacy engineer is to set policy within a company, with regards to privacy protection. More specifically, “We don’t make policy recommendations externally, we just do it for [ourselves] and we make cool tech that we think we can help set a higher standard for privacy.” (I4-T). In this way, a privacy engineer is perhaps a bit more locally positioned (i.e. within an organization) than a DPO, whose reach necessarily extends beyond the organization to the laws and regulations in question. I9-T validates the previous quote: “We’re the ones who define, dictate, and do privacy assessments.” These assessments, in turn, become the basis for design decisions.

The role of a privacy engineer is undoubtedly unique and dynamic. As a final description, and one that left quite the profound impression, “Privacy engineering is fundamentally dealing with science that has not yet been codified.” (I4-T). Alas, the field of privacy engineering has its work cut out.
6. The Structure of Privacy Compliance

6.3. Interactions

While the interactions between the parties involved in the privacy compliance structures have already been alluded to via the individual descriptions of each role, they are made explicit here. By doing so, the individual roles are described within an ecosystem, rather than as self-standing. Through this, the larger picture will hopefully become clearer via horizontal, vertical, and diagonal connections.

6.3.1. Technical-Technical

Before the influence of legal support even comes into play, the interviews revealed that much of the interaction regarding the technical measures for privacy compliance occurs within the technical sphere, naturally. It is in these technical-technical interactions that many of the technical roles described above operate in their daily capacities. Some of these interaction types are described now.

The first set of interactions occur “vertically” within the engineering side of compliance. A privacy engineer may not be “working directly with legal to do things, [but] still taking direction from [an] engineering manager.” (I1-T). This is validated from the statement of another privacy engineer: “Sometimes I’ll interact with a program manager or a technical program manager, if there is need, like maybe they have broader insight into a project that a given engineer doesn’t.” (I4-T). Privacy engineers aside, the privacy architects involved also have a “factual reporting line to the product management” (I2-T). In this way, one begins to see that much of the guidance and direction for technical decisions regarding privacy is handed down from direct managers within an engineering vertical. Specifically, “the head of the tech vertical will always get down to the cut and dry for us, which is directly asking legal questions.” (I1-T). In this case, the distinction between different levels of management is not made, and one can assume a traceable route to any particular level of the hierarchy.

Also included within the interactions with upper levels, but one that was mentioned explicitly on several occasions, was interaction with a chief (information) security officer. Whereas a “factual reporting line” was described for product management, “a dotted line” relationship exists with the chief security officer. Much in the same way, the work of an architect must ultimately be “validated or not validated, agreed upon with [the] information security officer” (I6-T). Thus, the interaction between architect and security officer seems to be truly vertical, whereas interactions between privacy engineers and management are more of the “diagonal” nature. This will be further explored in subsequent sections.

Of more of the “horizontal” nature comes interactions between privacy engineers and other parties. One privacy engineer is “in almost constant communication with either subject matter experts, software engineers, or both, because sometimes they overlap” (I4-T). The dialogue with these subject matter experts is important for privacy engineers to stay up-to-date on relevant topics, both technical and legal. Interactions with software engineers can be viewed as more of a “diagonally down” relationship, as privacy engineers provide the necessary guidance and policy for privacy-protecting systems.

A final important set of interactions within the technical sphere is interactions with peers.
within the same group or team. An illustrative example of these came from the interview with I4-T, who described a team of many privacy engineers, all of whom were specialized in something slightly different. Because of this, each member’s strengths could be drawn upon for the mutual benefit of all privacy engineers. These horizontal relationships, therefore, play a vital role as well.

6.3.2. Technical-Legal

It is in the interactions between the technical and legal sides of privacy compliance where arguably the most interesting relationships can be explored. As introduced in previous chapters, the very existence of a technical requirement for compliance to privacy regulations has brought together two inherently different fields, and more abstractly, two quite different ways of thinking. These relationships are introduced here, and there intricacies (and possible challenges) will be elucidated throughout the remainder of this work.

Starting from the non-management level of the engineering vertical, the main technical-legal interactions occur with the appointed Data Protection Officer. In the words of an architect, “Sometimes we interact with the data protection officer, when it’s about the specific interpretation of legal requirements or validating a certain technology fits to the requirement or not.” (I2-T). This description is very insightful in the way that it binds the interpretation of legal requirements to the validation of a technology. Precisely this illuminates the go-between role of the DPO. Another source of legal support for engineers, going back to the horizontal interactions described above, is described here: “Who do I go to with a legal question? Normally, I’ll ask senior experts, people who are privacy engineers, who are former lawyers, it’s probably my first pitstop.” (I4-T). The amount of privacy engineers fitting this description is certainly relatively low, but such a resource would undoubtedly be greatly helpful to a fellow privacy engineer.

Viewing this category from more of the legal-technical direction, the interaction between legal support (besides the DPO) and non-management technical parties seems to be of the rarest occurrences. I8-L mentions sometimes liaising with an organization’s structured IT or development teams, claiming “I can’t imagine how I would be able to actually do my work without kind of a real input from the IT team.” (I8-L). I16-L also mentions such interactions.

A set of interactions that takes place undoubtedly more often is the dialogue between legal teams and the technical leadership of organizations. Bringing the chief security officer back into the mix, one illustration of the technical-legal relationship from the legal perspective is as such: “We have a designated information security officer, who works with these issues from the IT side. And usually I share my findings with him, and he shares his findings with me. So we’re kind of communicating really, I would say, really well.” (I8-L). A similar level of communication is conveyed from an external DPO, who initially sets up an “at least two hour interview with the IT leader of the companies” (I12-L). Within such interviews and discussions, I16-L explains the type of information exchange within these interactions:

An initial interview with the lead stakeholders or I will seek employees of the organization to understand how does the data apply to the organization... so
that we get an informed and complete answer to certain queries... what are the practices and what are the best things they need to have... Basically, we interview with the stakeholders, may involve the sales team, the marketing head, or the finance side and etc, the procurement head or something like that. And the most important stakeholders which I feel, are marketing and HR... they are the crucial stakeholders which we feel ultimately for the privacy implementation. (I16-L)

This description also brings in other, non-technical stakeholders who are believed to be important to the process of privacy compliance. While these parties will not be focused on, they should nevertheless be included in the overall privacy compliance structure.

The final type of technical-legal interactions comes in the form of cross-teams, or cross-functional teams, a topic which came up in some interviews. These teams will typically consist of members hailing from different departments, including those that are more technically or legally oriented. While such a concept does not always exist, it certainly describes an interesting avenue for cross-disciplinary exchange.

6.3.3. Legal-Legal

A final category of interactions described in some interviews were those of the legal-legal nature. Again, while these are out of scope, they are only mentioned briefly here.

Outside counsel or even an external DPO may often work with the legal compliance team within an organization, serving a more advisory or guiding role. Similarly, an internal DPO may seek consultation from an external consultant.

An interesting example comes out of the interview with I14-L, with the idea of a “Data Governance Council”. While this is not a purely legal team, it is placed under the legal-legal category. Specifically, this council is “is more of an independent board of senior leadership. So if anything ever needs to be flagged from both business and clients and legal it gets escalated them to them, and they can make more of the business related approaches to risk” (I14-L). Certainly an interesting sub-structure, but something that is not widespread adopted, as far as can be determined from the interview findings.

6.3.4. Documentation

Although not the main focus of this thesis, it was interesting to ask interviewees about the artefacts, or simply documentation, that they use in the process of privacy compliance. While this was an explicit question in the technical interviews, some legal voices also chimed in. Learning about some of the documentation in play could be useful to understanding the overall structure of privacy compliance.

What became clear is that the documentation involved is certainly not the same across the board. Serving in more of an auditor role, I1-T regularly utilizes “a large document that categorizes a few 100, almost 1000, just different companies [all the third party services].” For an architect, a document that becomes useful is “an overview of requirements. So you could say it’s a checklist, but then how you fulfill the requirements, that’s pretty much up to the
business unit.” (I2-T), which also brings the idea of a business unit into consideration, which for the purposes here, is blended into the product team. Possibly one of the more relevant artefacts pertaining to privacy compliance is elaborated upon by a privacy engineer:

Most privacy review teams use something called a privacy design doc, which will literally go through chunk by chunk, how an overarching family of products goes through every category of data protection. (I4-T)

Particularly with the idea of a “privacy design doc”, such a process involves a collaborative effort between multiple parties in the privacy compliance process. Because of this, it illustrates a dynamic process which could be quite promising for more widespread adoption.

Another large role of documentation within the privacy compliance process comes with its use in the risk assessment phase. One specific example of this process is described in I6-T’s explanation of a

CIA analysis report. And one important thing that they capture is something called CIA, which is confidentiality, integrity, and availability, and this score for each of these three things... for these three categories, they provide a score, or ranking. For example, they have a ranking system of 1-2-3. And lower the score higher the confidentiality.

This analysis seems to be a crucial stage of product development that occurs before any implementation is performed, highlighting the necessity of a thorough assessment before any data processing endeavor is undergone.

On the legal side, the documentation involved comes more in the form of support documents that are meant to guide clients in the process of privacy compliance. One interviewee who serves in an external role states: “We provide checklists for companies, and you work your way through that list.” (I5-LT), and the statements from other legal interviewees seem to be in line with this. One unique statement that actually rings true for much of the insights provide about documentation on the legal side comes with: “My team is so old school, we very much like [physical] documents.” (I14-L). It could even be argued that for all groups involved, technical and legal, much of the documentation is very much of the physical medium. Further investigation into this matter could be useful to determine the benefits and potential areas for improvement here.

6.3.5. Liability

One final supplementary area of investigation, comprising of a single question in the technical interviews, asks to whom the liability falls for privacy compliance. While some interviewees could not confidently respond, three succinct answers shed some light on the answer:

The product organization has to make the go no-go decision at the end of the day. (I2-T)

Every single person at the company. (I4-T)
Privacy compliance, as referring to privacy regulations, that is always legal, in my experience. (I9-T)

The differences here are quite striking, suggesting that liability for privacy compliance is not uniformly held by any one party in the industry. Moreover, one can argue that it speaks to the ever-evolving (and rather “new”) nature of data privacy compliance. Once again, another very intriguing area for further investigation.

6.4. The Privacy Compliance Structure, Visualized

As a final step for answering Research Question 1, a diagram of the privacy compliance structure has been created. This serves as an attempt both to summarize what was discussed in this chapter, as well as to illustrate the placement and direction of the roles involved and the interactions that occur. While this picture might not be completely comprehensive and contains some simplifications for the purpose of generalization, it is to the extent of the author’s knowledge an accurate representation of the structure of privacy compliance today.

6.4.1. The Diagram

Figure 6.1 contains the above-explained diagram.

Explanatory Notes

Some general notes and clarifications are in order for explaining the significance of the shapes and symbols used in Figure 6.1.

- **Rounded rectangles** denote a particular role involved in the process of privacy compliance. The rectangular containers under which they fall can be seen as departments and/or general group descriptions.

- **Uni-directional (solid) arrows** denote a “reporting line”. Solid arrows are “factual”, while **dotted arrows** are indirect reporting lines. The one exception here comes with the arrow connecting Privacy Engineers to themselves – this represents internal interaction.

- **Bi-directional (solid) arrows** denote two-way interactions, or dialogues, rather than hierarch-ical reporting lines. Whether these arrows are vertically or horizontally portrayed is indeed significant.

  The **bi-directional (hollow) arrows** located on the top-right corner of Figure 6.1 serve two purposes: (1) the same as bi-directional solid arrows, and (2) to denote that sometimes these positions are held by the same person. For example, an external consultant may also serve as an external Data Protection Officer for an organization.

  Finally, the **sketch-filled rounded rectangle** in the center of the diagram denotes the approximate position of the group; furthermore, this may not always exist at all. The location must be kept approximate due to the dynamic, hybrid nature of the group. Specifically in the case of a cross-functional team, this is certainly the case.
6. The Structure of Privacy Compliance

Figure 6.1.: The Privacy Compliance Structure
7. Challenges

This chapter comprises of the crux of the investigative work for this thesis research, which is to identify the practical challenges in the implementation of technical measures for privacy compliance. The challenges introduced in the subsequent sections arise from a qualitative analysis of the interview transcripts, as outlined in Chapter 4. As it turns out, the challenges can be broken down into four major categories, relating to: the technical-legal interaction, PETs and technologies, organizational factors, and general challenges. Chief among the insights brought to light here are that the factors influencing the implementation of technical measures without a doubt include, yet extend quite far beyond the technologies themselves, revealing a dynamism and interplay that will be expounded upon in the following. As a general note, the purpose here is to introduce and outline each identified challenge. The relevance and general acceptance of each challenge will not but discussed here, but rather will become the task of the next chapter, as part of the quantitative analysis. Furthermore, in no way is each introduction purported to be a complete and exhaustive synopsis of the themes within; rather, they hopefully provide a succinct introductory summary, upon which further analysis and research could be performed. The challenges are supported by direct quotes from the interviews, which serve as the basis for all identified challenges and upon which the author has built the discussion surrounding each one.

7.1. Setup

Each challenge category will be introduced and discussed in a structured fashion. Firstly, an overview of each category will be provided in the form of a table. This table will include each challenge with their appropriated code, brief description, number of interviewee mentions (mentions), and number of overall relevant mentions (occurrences). This distinction here should be made clear: mentions denote the number of unique interviewees that brought up a particular challenge, while occurrences denote the number of unique times this topic was brought up. Occurrences will always be greater than or equal to mentions, for example if a single interviewee brings up a challenge during several different points in the interview. The decision as to what amounts to a unique occurrence is left to the author’s discretion, but it is generally defined as a distinct thought.

The second part of each challenge category comes with the discussion of the individual challenges themselves. In some cases, these discussions are preceded by a particularly impactful or meaningful quote, which is meant to prelude the following discussion. In all cases (minus one), though, the discussion of the challenge will contain one or many direct quotes, so as to ground the particular argument.
In the final section of each challenge category, a mapping of interviewees to the challenges is illustrated. In particular, this takes into account the mentions and occurrences as described above. By doing this, such a mapping will show the relative strength and prevalence of the identified challenges among the interviewee pool.

Without further ado, the challenges.

### 7.2. The Technical-Legal Interaction

Perhaps at this point it has already become clear that the process of data privacy compliance inherently requires the collaboration of technical and legal forces. It is precisely this point that was hopefully elucidated best by the discussion in Chapter 6. Now, the concept of technical and legal experts working together is certainly not something novel; moreover, one cannot claim that modern privacy regulations has “created” this dynamic. One might imagine, however, that with the rather sudden rise in the implications of an every-growing attention paid to data privacy (regulations), the technical-legal interaction has become more necessary (and commonplace) than ever. Exactly because of this urgency, and of course the fact that the two fields in general possess inherent differences, one can reasonably expect challenges to exist, i.e. that a perfect harmonization of the two parties does not come immediately. For this reason, the discussion of challenges begins here.

#### 7.2.1. Category Overview

This category contains 8 challenges, which are summarized in Table 7.1.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Mentions</th>
<th>Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1.1</td>
<td>Rare direct interaction with legal</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>C1.2</td>
<td>Interaction with legal is frustrating / not desired</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>C1.3</td>
<td>Deadlock between technical and legal mindsets</td>
<td>9</td>
<td>14</td>
</tr>
<tr>
<td>C1.4</td>
<td>Technical knowledge lacking on the legal side, and vice versa</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>C1.5</td>
<td>Lack of technical input in privacy compliance</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>C1.6</td>
<td>Technical-legal gap is desired</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>C1.7</td>
<td>Lack of interdisciplinary / cross-functional teams</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>C1.8</td>
<td>Regulations leave much up to interpretation</td>
<td>10</td>
<td>11</td>
</tr>
</tbody>
</table>

Table 7.1.: Challenge Category 1, The Technical-Legal Interaction
7. Challenges

7.2.2. The Challenges

C1.1: Rare Interaction

*What we see is that there is a huge gap. And this gap is because the informatics guys don’t talk to lawyers, lawyers don’t talk to the informatics guys.* (I10-LT)

To begin the discussion regarding challenges existing within the technical-legal interaction, one may start with the cases in which this interactions happens rarely, or not at all. In a process where interdisciplinary communication can most likely come as a benefit to all parties involved, the lack of this dynamic can create challenges of mutual understanding.

The first aspect of this challenge can be viewed from the technical perspective. As someone working on the “technical side” of privacy compliance, it may still be the case that most or all of the guidance and direction is coming down from within the *engineering vertical*. For example, I1-T states that “I’m not working directly with legal to do things, I’m still taking direction from my engineering manager.” This sheds light on the privacy compliance programs of some organizations, where the engineers involved receive vertical direction, rarely directly communicating with legal entities.

Another way in which rare interaction between the technical and legal sides occurs comes not by the frequency of interaction, but by the manner in which interaction is initiated. An interesting insight comes from another technical interviewee, who explains “I almost never actually interact with the legal team, because if you have to escalate something to legal, it’s generally pretty serious.” (I2-T). In this case, one can extrapolate how in this particular compliance structure, interaction with legal is “reserved” for rather serious cases.

A legal perspective chimes in with the claim, “There needs to be more communication... before starting any exercise, legal should be consulted so that they don’t face any difficulties for data privacy implementation.” (I16-L). Implicit within this statement is an observed lack of communication, and this relates back to I10-LT’s quote above. Another important insight to draw from I16-L’s statement is the perceived need for sound communication between the two sides in order to avoid “any difficulties”. In this way, this challenge is also validated from the legal position.

In summary, it can be seen that interaction between the technical and legal proponents of privacy compliance does not always occur with great frequency. Furthermore, one can assume that for some cases, such interaction would indeed be of benefit. This, though, may not always be the case. While the actual implementation of technical measures may predominantly reside in the technical realm, their clear tie with legal regulation necessitates a mutual understanding between technical and legal colleagues. Where this understanding is not fostered by regular interaction, challenges may occur.

C1.2: Sub-optimal Interaction

Building upon C1.1, the discussion moves on to the cases in which such interaction does indeed occur, but in a somewhat sub-optimal manner. Interestingly enough, such a challenge
was mainly brought up in interviewees with technical experts. An added complexity comes with the question of whether more interaction is desired.

The interaction between the two sides can be viewed as non-desirable in the way that finding an initial mutual understanding is difficult. According to the I2-T, “The most complicated part is always initial alignment.” This is echoed and expounded upon by a legal interviewee, “Some tech guys do not like to talk with us, they don’t want to show the technical things. They get scared, why will we share our technical specifications of the organization.” (I16-T). While this statement may refer back to a specific case or cases, it gives way to a general difficulty in what I2-T calls an alignment. In a nutshell, the demonstration of sound data privacy compliance requires that technical parties can illustrate the inner-workings of their systems, particularly the data flows, are in compliance with regulation. In turn, legal parties must be able to communicate what exactly in these regulations is relevant, and in what way they must be followed. With this in mind, getting on the same page can be quite a challenge.

Another way in which sub-optimal can be defined is frustrating. I1-T puts it simply, “I think that the biggest challenge is with the legal side. As I said, it’s too convoluted.” This statement came along with an anecdote of how a rather simple compliance question was met with “legal jargon”, of which this particular interviewee found rather complicated. To further complicate the matter, another technical interviewee takes one step further in saying,

I will say that lawyers also do not have a good enough technical understanding and some of these cases to be able to make an assessment of compliance because they didn’t understand at a technical level, the systems and were unwilling to reconsider or consider some of the technical things in a way if they did not sort of see it first. (I9-T)

This statement not only supports I1-T statement (in a somewhat reversed fashion), but also serves as a great introduction to a subsequent challenge, namely C1.4.

The main question raised by this challenge is what can be done to remedy sub-optimal interaction. This is something that will not only be discussed here, but it will resurface at several points in later challenges. A “simple” solution could be more interaction, whether that be through regular meetings, calls, etc. This suggestion was seen as non-productive by I4-T, responding that “they’re [legal] not going to know how to do what I do.” An answer somewhat more in the affirmative comes with: “Yes, and no... it of course adds that much more hurdles that you have to jump... That’s why I said no, in that respect, but yes, in the respect of it really helps to clarify specific doubts later.” (I6-T).

One can see a somewhat double-edged sword in the promotion of more interaction between technical and legal forces. On one hand, this can be perceived as a “hurdle” in the way that it enforces communication between two fundamentally different parties. On the other hand, such interaction, when effective, can serve to clarify doubts and avoid difficulties down the road. In this way, the complexity of this challenge is revealed.

C1.3: Technical-Legal Deadlock

We don’t understand each other. (I14-T)
The quote above, taken perhaps a bit out of context, is profound in the way that it succinctly sums up the argument of this challenge. Specifically, I14-T explains how engineers with technical background and lawyers with legal background must essentially come to the same table that is privacy compliance, and they are expected to “speak the same language”. In reality, this does not always proceed smoothly. As such, this challenge explores a unilaterally perceived deadlock between technical and legal mindsets in the process of privacy compliance.

The acknowledgment that there exists inherent differences between the technology and legal fields is not new. In [47], Gifford describes the relationship between law and technology as “both simple and exceedingly complex”. Technology aims to “develop as ways are found to produce new results or to produce old results using fewer or less costly inputs”, while the main premise behind law is “to exist as a set of rules adopted by a society’s governing institutions that are applicable to all of its inhabitants.” Even with these two rather straightforward definitions, it might not be immediately clear where is the common ground. This fact certainly plays into this and several other challenges presented in this work.

This challenge arises out of a dynamic to which has previously been alluded in this work. Specifically, the new wave of data protection, regulations thereto, and the requirement for sound technical measures has brought together two disciplines that have inherently different training, language, responsibilities, and ultimately, cultures. This is certainly reflected here:

...the biggest challenge here is the mixing of those two disciplines because historically, IT and legal have not talked to each other and they didn’t have to, and data protection and privacy is a very strong motivator to do that. (I5-LT)

Even beyond this inherent “historical” aspect, the challenge also lies within the way in which both sides operate on a day-to-day basis. At a foundational level, there is “a different type of language that lawyers speak, than the technicians speak” (I7-L). This can be meant more abstractly, but also concretely. For example, I8-L claims that this challenge can “sometimes comes from different understandings of the same concept.” A concrete example mentioned in several interviews is the technical vs. legal definition of an incident or of consent. However menial this may seem, it sheds light on different operational structures between the technical and legal sides.

Another source of deadlock seems to rise out of the challenges discussed in C1.1 and C1.2. An interesting dynamic is illustrated by I8-L:

I think that’s also something that for a lot of companies is missing, because these two teams maybe don’t communicate between themselves. Or, for example, the legal team just kind of poses some requests or requirements. And then the IT team does not know how to deal with that.

This interviewee goes on to explain how this dynamic can lead to a certain inflexibility between the two sides of privacy compliance, even to “backlash”. I16-L also explained a similar challenge, where the technical team and legal team were essentially out of sync, with “no communication with the legal team”.

51
7. Challenges

The challenge portrayed here is not meant to suggest that the collaboration between technical and legal experts is impossible. Indeed, some interviewees also shared experiences of great and seamless communication between the two parties. The core of this challenge, though, truly lies in the different perspectives and backgrounds offered by the various persons involved in the ultimate implementation of technical measures for privacy compliance. I16-L explains this in an extremely insightful way, talking of a “silver lining” between following the “spirit of the law” and “at the same time [understanding] the practices of the organization.” All of these factors certainly have an effect on the implementation of technical measures, before the actual implementation itself can even take place.

To summarize the discussion of this seemingly crucial challenge, as well as to motivate further discussion, another profound quote is left below:

*It’s really a interdisciplinary challenge... Because if you take a stock informatics person, you confront them with the legal challenges. They are mostly very, very good at interpretation of concrete texts, you give them an article, they get it or they get it even better than any lawyer, but they miss to see the relations that this one article can have in the entire legal system, which is a value system, which is not as precise as informatics.* (I10-LT)

C1.4: Lack of Domain-specific Knowledge

Challenge C1.4 once again segues very well from the previous challenge because it points to perhaps one of the most important factors contributing to a potential deadlock. Namely, this factor is a lack of domain-specific knowledge in the individual persons involved with privacy compliance. Specifically, this refers to domain-specific knowledge of the *other* parties involved, keeping in mind the very interdisciplinary nature of this field. It must be made clear upfront that any perceived lack of knowledge is not the fault of any party involved. After all, one cannot reasonably expect engineers to be licensed lawyers, and vice versa. The challenge, therefore, merely highlights the state of things, however inevitable they may be.

Taking one step back, it should be noted that the study of this sort of domain-specific knowledge has certainly been investigated, particularly on the legal side. As it turns out, very few law schools offer courses on technical subjects [48], even in light of the current wave of LegalTech. This could certainly be a source of the lack of knowledge described in this challenge. On the flip side, little to no research has been performed investigating the degree to which legal knowledge exists on the technical side, to the best of the author’s knowledge. And this is understandable, as it is presumably much rarer the case that an engineer must be somewhat proficient in legal matters. Unfortunately (or maybe fortunately), the process of privacy compliance is very much so one of these cases.

It became clear from the interviews that members from both the technical and legal sides were lacking in the knowledge of the other, self-admittedly. One technical interviewee even interestingly expressed, “If I would go to university again, I would love to study law... Because I feel like one part of the language is missing. Now, I know the computer science. Sometimes I would like to know the legal side.” (I2-T). This is not only intriguing in of itself, but it introduces a theme that surfaced in several interviews in one way or another, and that
is the wish for a “happy medium”, so to speak. This means in particular the existence of a person within the privacy compliance process who is fully proficient in both the technical and legal aspects. Surely this is rather ideal, at least for the moment, but an excellent goal nonetheless.

The perceived shortcomings in domain knowledge was also described for the legal proponents of the process. From a technical perspective, “a lot of lawyers might have some technical trouble understanding storage infrastructure, or understanding a machine learning algorithm.” (I4-T), given as an example. This was partially validated in a statement by a legal interviewee, in relation to a situation where Privacy-Enhancing Technologies were in play: “I couldn’t recommend something [about PETs]. Because I didn’t know.” (I12-L).

While this can certainly be a challenge for technical measures, the question becomes what can reasonably be done to improve the situation, outside of an engineer acquiring a law degree, and vice versa. Looking at the current state of affairs, I2-T predicts that “you will need to factor in legal advice a lot more in future projects from a technical standpoint.” With this in mind, however, it became apparent that involvement from legal experts in more technical matters is currently limited. One interviewee says, “I never touch systems of the clients, never. Because that’s not my job.” (I12-L), which of course is reasonable to understand, but it still portrays a gap. Taking one step further, I3-L holds that, “I don’t really care about the technology, frankly, the technology today is not going to be the technology tomorrow.” Not only does this echo the previous statement, but it also introduces a sub-challenge, namely that the ever-evolving nature of technology makes obtaining domain knowledge a bit of a Sisyphean task for the legal side. One can extrapolate from here and claim the same for the technical side, as the field of law (i.e. privacy regulations) is also rapidly changing. Thus, the challenge is exacerbated.

Particularly with data privacy compliance and the implementation of technical measures, a topic that came up in many interviews is that of data flow. In a potential sea of technical specifications, the seeming most crucial information to share between the technical and legal sides is, how is the data flowing? This, as I14-L puts it, is key to “understand the whole story”, or similarly “to understand the whole perspective and how the business conducts and how the data flows” (I16-L). In return, technical players “need to know enough to be able to ask the questions” (I3-L), meaning that they should be aware enough of legal aspects to be able to ask for legal help in a knowledgeable way. Again, this goes back to the need not necessarily for more interaction, but perhaps better or more informed.

A final closing aspect of this challenge, which is one that stems from the opinion of one interviewee, definitely has merit to be included here. This is that:

It’s a lot easier for a technical person to learn the law, like to do training to understand certain aspects of legal regulation, than it is for a lawyer to understand the technical requirements of a system or the system design. (I9-T)

It is important to note that this was qualified with the explanation that this is not necessarily because the legal side is “easier” to comprehend, but rather due to the availability of learning resources, such as certification programs. Therefore, it is paramount to acknowledge the existence of this gap; furthermore, this in particular opens up wide avenues for further work.
7. Challenges

C1.5: Lack of Technical Input

*Less lawyers, more technicians.* (I7-L)

The challenge described here is unique in the way that it certainly pertains to technical measures, yet it extends beyond the technologies themselves to the ecosystem of privacy compliance. In particular, the challenge in question refers to a perceived lack of technical input, i.e. input from technical experts, in the discussions surrounding compliance and its requirements. As such, challenge C1.5 can be viewed from two perspectives, a static one and a more dynamic one.

The first perspective, the “static”, looks at the current state of affairs, and this is something that will be covered in greater detail in C1.8. Talking about modern privacy regulations, I14-L sees that a “huge technical aspect there is missing”. This was expressed in other words by a technical interviewee when discussing the technical nuances of some of the systems in question: “laws are not aware of these differences. So we’re in this weird bind.” (I9-T). These both essentially indicate a situation where the regulation itself requires a technical aspect for compliance, yet the guiding backbone is not there. Put in a more cynical, but telling, way: “The law is administered by lawyers. And lawyers have no clue about data protection, about informatics.” (I10-LT). Thus, the static view reveals a certain challenge.

The “dynamic” perspective is one that is perhaps more relevant to this particular challenge. What is meant by this dynamism is the way in which technical input (or lack thereof) has shaped the evolving field of privacy compliance. Looking at the current discussion around this matter, one legal expert sees a potentially unwanted divergence:

...rather than having the discussion around what [technical] measures can be considered sufficient, they’re having that legal battle around - do I need a legal basis?... So I would wish that the discussions with the data protection authorities would be less legally driven, rather about technology. (I7-L)

Here, a challenge with the implementation of technical measures is quite clearly spelled out, in the way that this process is currently very legally-based. Instead, a desire for more technical input, i.e. for the discussion to be centered around “the technology”, is expressed.

Continuing with the dynamic metaphor, the challenges regarding the lack of technical input also have pervaded the development of the field, that is how privacy compliance will look moving forward. The following two quotes from a single interviewee illustrate this dynamic in distinct, yet similar pictures, in a way that the author could not simply write himself and should not have paraphrased:

If you look, for example, what the privacy bodies are doing on the European level, they don’t have that many links with IT issues, they are really focusing on the legal perspective... but they are not addressing these IT security issues as well. So it’s kind of like the IT side is really pushing towards GDPR. And instead of going towards that, the legal side is just kind of staying in their legal corner. (I8-L)

It’s weird that it’s kind of like a body with two feet, and the feet are going in different directions, not moving in sync. I think that it’s a problem and how it’s...
been all the time with GDPR. And it’s focused a lot on very specific legal issues. But when it comes to security issues and technical security issues, it’s just kind of ensuring adequate measures. That’s it. So it’s just frustrating. (I8-L)

In order to digest these quotes a bit, it may be useful to draw the connections. In both, a clear distinction between the technical and legal sides of privacy compliance is made, portrayed by “corners” or “a body with two feet”. The way in which these sides are “out of sync” is based on the focus of both entities. While the legal side believes that a legal debate (referring back to I7-L’s quote) is the right way moving forward, the technical side proceeds forward in the realm of security (and one can assume privacy) issues with the development of “compliant” systems, with no clear parallel between the two. At the core of this issue lies the lack of technical input.

Looking forward, it is apparent that something will be required to realign the two tracks, or rather to get the two sides “back into sync”. Clearly, “a lot of what data protection law is becoming is that it’s going to be influenced by people with more technical background.” (I14-L). Exactly how this looks and will be carried out is up in the air, though. Nevertheless, one cannot deny both the lack of technical input in the discussion and the need for such involvement going forward.

The one way I see it is tech is driving a lot of the new changes in privacy. And it’s not enough for it to just be a legal focus without consulting with tech, I think it needs to be a mix of the two, because the two kind of balance each other out, because that’s what privacy is becoming. (I14-L)

This sentiment will without a doubt be echoed at several subsequent points in this work.

C1.6: The Technical-Legal Gap: An Opposing View

I do wish more people appreciated that gap, that there there is a fundamental gap. Like the fact is that gap is okay. (I4-T)

This particular challenge will only be covered in short, as it is mainly a challenge arising out of one interview. Its importance and general relevance, though, led to the creation of a separate challenge.

The challenge re-introduces a theme that has already appeared often in this challenge category, the idea of a “gap” in the technical-legal interaction. Implicit in this challenge is the acknowledgement, once again, that the gap is indeed “fundamental”, since two inherently fields of study (and practice) are brought together with the process of privacy compliance.

Specifically, this challenge is brought up not only because of the fundamental gap, but also the dynamic introduced when this gap is desired, or when it is the standard “way things are”. To provide a legal voice to this debate, a legal interviewee provided in response to a question about technical knowledge: “I have an understanding on how [the systems] work. But I’m not a technician at the end of the day.” (I7-L). One may argue such a sentiment also speaks for a certain acceptance of the technical-legal gap.
7. Challenges

A further discussion and analysis of the more ingrained challenges (and potential merits) of this gap will not be performed here, as it is out of scope. Works such as [15] provide an excellent template for such analysis, of which there certainly remains much work to perform going forward.

C1.7: Lack of Interdisciplinary / Cross-functional Teams

*That is the most important part as far as privacy compliance is required because both things, the tech and legal things, go hand in hand to privacy compliance... it is very rare to find, but it would be very ideal if tech and legal worked side to side.* (I16-L)

The argued challenge here is self-explanatory, and while the introduction will be made in this section, the topic will be discussed in detail in Chapter 9. If one recalls the privacy compliance structure presented in Figure 6.1 of Chapter 6, one of the biggest question marks left in the picture is the presence of cross-functional teams. These interdisciplinary units, although mentioned in some units, are by no means standard when it comes to privacy compliance. The challenges that lobby for more of these teams are outlined in the following.

A schism created by the different technical and legal mindsets has already been mentioned at length, but sometimes the physical divide can also add to the challenge. Where cross-teams do not exist, communication between people with different roles and functions leads to an extra “hurdle”, to refer to the terminology used in a previous quote. Such separation strengthens the argument for interdisciplinary teams: “We need these guys [legal] to talk to the IT department. And that needs to be in the same place.” (I5-LT). Note that in the discussions here, *distance and location* are meant to be relative – “same place” naturally need not be literally the same room, but as one can imagine particularly in large organizations, not being “co-located” may mean a relatively large distance between teams in the privacy compliance structure.

The main point and goal of these teams is communication. A lack thereof is what can lead to many of the challenges discussed in this challenge category. I9-T agrees: “I think it requires cross communication and processes to a large point.” From a legal perspective, this communication also is highlighted as being crucial:

The main point would be just communication between the teams, the legal team to really understand what the IT team has, for the IT team to understand what are the legal requirements, because I think that is where there’s a lack of communication. (I8-L)

Particularly in this case, the communication *between teams* is described. Drawing upon the insights from other interviewees, this kind of communications would most likely be enhanced if it took place *within a team*, specifically a cross-functional team.

Preliminary research found in the literature would seem to agree with the need for interdisciplinary teams. One such advocate is found in [49], which promotes hybrid technical-legal teams for the purpose of determining how certain technical measures fall under the requirements of regulations such as GDPR. One unique case also comes with joint research groups,
which blend informatics with applied law, such as the Information Law for Technical Systems and Legal Informatics (Compliance) at the Center for Applied Law (ZAR) at the Karlsruhe Institute of Technology [50]. Such dynamic groups could possibly be of great benefit if also found in practice.

Exactly how these teams would be comprised and at what place in the privacy compliance structure they should be located is outside of the knowledge of the author; furthermore, the general lack of these teams in the industry may suggest that no “correct” answer actually exists. Nevertheless, the challenges that lead experts to promote these teams indeed exist; the main benefits of interdisciplinary teams in addressing some of these difficulties will be covered later.

C1.8: Interpretation of Regulations

Compliance is kind of, it’s difficult because sometimes you’re operating in a bit of a gray area, you’re not quite sure because legislation sometimes is a little vague, and you don’t have much guidance. (I14-L)

Because if a regulation doesn’t provide a good blueprint, then engineers are necessarily going to fill in a gap with what they think is privacy protection. (I4-T)

The last identified challenge of this category is one that lives on the fringes of the “technical-legal interaction”, and in fact it speaks very much also to the privacy regulations themselves. Challenge C1.8 is arguably one of the more prevalent of this category, having been brought up in the large majority of the interviews. Indeed, one of the main original motivations of this thesis was grounded in the idea that the makeup and structure of today’s most predominant data privacy regulations may, however inadvertently, create challenges for the implementation of technical measures.

Looking at this challenge requires first looking at the nature of these technical measures. This phrase was specifically motivated by its use in the GDPR, and is used generally to define the required measures in order to safeguard data and protect privacy, and ultimately to demonstrate compliance. It is without a doubt that this phrase is vague, but for reason. Taking GDPR as an example, it “mentions technical measures, which were deliberately left open, because technology changes so fast, they have left the generic and said state of the art.” (I5-LT). From a lawmaker point of view, this certainly is logical, for as to prescribe the use of specific technologies would certainly render regulations out-of-date quite quickly, perhaps even before they can be ratified. The vagueness of GDPR as it pertains to technical measures is also acknowledged in research, such as in [51] or [52].

Another insight into the nature of technical measures is related to the previous, but brings in a cultural aspect. I3-L says, “I think the technical measures is the GDPR attempt to sort of get all of Europe closer to the American approach, to say we can’t keep dictating to you how you do these [technical measures], because they change too often.” To bring this statement more into context, the interviewee introduced two types of approaches for taking technical measures: (1) the letter of the law approach, named the “European” approach, and (2) the risk
management approach, named the “American” approach. The former proceeds by following
the law as exactly as possible, while the latter interprets the technical measure requirement as
a case-by-case prescription, which needs to be determined via a risk assessment. More on
this later.

Although it is interesting to observe different perceptions of the nature of these technical
measures, it is more pertinent here to analyze how this requirement is reflected and affects
privacy compliance in practice. From a technical perspective, “there’s a lot of responsibility on
the technical teams to do their homework.” (I2-T). What this means can possibly be explained
better by the second quote at the beginning of this section.

The implications of this for the creation of compliant systems were also made clear,
introducing some challenges. I8-L sums it up in this way:

In a sense, it creates a lot of issues and a lot of problems and a lot of headaches.
Basically, I think it’s what you have to do to ensure that your technical and kind
of IT structures are secured enough. But the level which you have to ensure its
adequate level, that is kind of tricky to understand.

This points to the core of this challenge, and that is the question of interpretation: to whom
falls the responsibility? I2-T might say the technical teams, but the answer is not clear.
Furthermore, the ability to measure privacy compliance is lacking:

Typically in organizations, they don’t have really a way to measure, we are good,
we are in the green zone, or we taking unreasonable risks, and we’re totally in the
red zone. (I7-L)

The idea of being unable to measure one’s compliance also falls under the challenge of
interpretation. As interpretations can be different even when the “interpreter” is defined,
herein lies the challenge.

The process of interpretation can also be convoluted. Ultimately, it “requires [an organiza-
tion] to actually do an assessment to determine what regulations and sort of legal liabilities
are in place. And that one gets a little more interesting or complicated.” (I9-T). Here, it is
meant that the assessment itself can be complicated, but even after this is performed, the path
might also not be crystal clear. Regarding technical measures, “it’s a really wide range of
things you can do, it always depends on which data categories your processing.” (I12-L) – yet
another “it depends” answer.

A few notes to summarize this final, important challenge. It is not in the purview of this
thesis or of the author to criticize modern privacy regulations; moreover, this is not at all
the intention. Many would argue that such regulations must be structured the way that they
have been (covered in Chapter 10). The fact remains that the requirement for sound technical
measures, no matter how coherent or not legally, must be interpreted and realized in the
technical realm – and it is here that challenges may arise. In the end, this specific challenge
ties into the concept of technical-legal interaction in the manner that it highlights the interplay
between regulations, regulators, legal entities, technologies, and technical entities. In this web
of interactions, there is bound to be some difficulties, but the discussions in Chapter 9 will
look at the challenges as an opportunity to optimize the process.
7. Challenges

7.2.3. Summary

The challenges in this category revolve around the main set of interactions that need to take place in order to exact proper technical measures for data privacy compliance. Instead of focusing on the technical measures themselves, these challenges focus instead first on the technical and legal people and processes surrounding them. Among these challenges are included the themes of rare or sub-optimal interaction, inherent differences, missing knowledge, and the question of interpretation. In turn, a call for a better analysis of the technical-legal gap, creation of interdisciplinary structures, and optimization of communicative channels can be seen. The prevalence and relevance of these eight challenges will be further analyzed in the next chapter.

Mapping

As this is the first mapping (each category will contain one at this point), the purpose and significance of symbols should be explained. The mapping is meant to map interviewees to each of a particularly category’s challenges. This is certainly not to quantify each individual’s contributions, but rather to show where emphasis was placed, and considering each interviewee’s background and line of work, it can be particularly interesting to investigate this emphasis.

In order to best illustrate this mapping, a spot matrix was chosen as the method of visualization. In this matrix, each “cell” contains a particular symbol, which indicates the number of mentions of a particular challenge. As the maximum number of mentions for a single challenge from an interviewee was either three or four, this largest symbol represents this.

One final note pertaining to this and the subsequent spot matrix mappings is that I13-T is not included. This is due to a technical problem during the interview which prevented recording, and as a result, no transcript could be used during the qualitative analysis.

The mapping of Challenge Category 1 is presented in Figure 7.1, which shows a fairly uniform distribution of technical and legal mentions.

7.3. Technologies

In light of the technical measures in question, the second challenge category now looks at the technology itself, and moreover, some existing barriers to the adoption and implementation of them. Specifically, an emphasis will be placed on Privacy-Enhancing Technologies (PETs), introduced in Chapter 2 and discussed further in Chapter 3. Indeed, as early as 1997, the utilization of Privacy-Enhancing Technologies was called for, specifically in the light of increasing privacy concerns at the dawn of the Internet [53]. The rise in research interest for this specific class of technologies certainly speaks to their promise, yet the question remains of what is their place in the process of privacy compliance. Additionally, how PETs relate to modern privacy regulations must also be investigated. Beyond these PETs, challenges within this category expose broader hindrances to privacy compliance, once again bringing the context into play, rather than purely the technologies themselves. It should also be noted
at this point that this particular challenge category contains the least number of supporting quotes, due to the fact that not all of the interviewees could speak knowledgeably to the technologies in question, specifically PETs.

### 7.3.1. Category Overview

This second challenge category includes 10 challenges, indicated in Table 7.2.
7. Challenges

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Mentions</th>
<th>Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2.1</td>
<td>Lack of a proper characterization of PETs</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>C2.2</td>
<td>Level of implementation depends on a company’s resources</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>C2.3</td>
<td>Difficult to communicate PETs</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>C2.4</td>
<td>No mapping of PETs to regulations</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>C2.5</td>
<td>Need for better education on PETs</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>C2.6</td>
<td>Lack of technical literacy</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>C2.7</td>
<td>Lack of a technical framework for compliance</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>C2.8</td>
<td>Companies implementing PETs are not rewarded</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>C2.9</td>
<td>The technologies are there, but the awareness isn’t</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>C2.10</td>
<td>Privacy compliance doesn’t motivate the innovation of technology</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 7.2.: Challenge Category 2, Technologies

7.3.2. The Challenges

C2.1: Lack of Proper Characterization

The first challenge in the technologies category is aimed directly at the nature of Privacy-Enhancing Technologies, in what is called a lack of “proper characterization”. This definition is multi-faceted, summing up to the general notion that while the motivation behind PETs is sound, its usability, understandability, and relevance to regulations is not quite clear or well-defined.

Looking at the former two aspects there, concerns regarding applicability to industry in a usable and understandable way are certainly grounded. Even from a technical perspective, “some of them [PETs] do really important and really good things, but some of them are very much too academic or not, not set up for real world use cases.” (I9-T). Not only is this something that has been addressed in the literature, such as in [54], but it is also a fact that will play into several of the other challenges in this category.

With this in mind, one must also consider how PETs may be viewed from a legal point of view. Similar concerns are expressed from a legal interviewee as those from above:

First of all, how complex is it? Because this defines which clients I can offer this... for me, I have a little bit of a technical background, but for me, ease of use is the most important, first how to use it. Is it self-explaining, is it very difficult? (I12-L)

In the case where a legal expert involved in the compliance process does not possess any technical background, these questions might become even more complex. Looking again at the concept of ease of use, this is arguably not one of the current strong points of PETs, suggesting a very important path for future work.

What this initial investigation into PETs ultimately reveals is what is meant by a lack of a proper characterization. The “academic” nature of them definitely contributes to this lack,
but the main driving force is introduced by I2-T: “Sometimes I would wish for automation when it comes to deciding how to characterize certain tools.” This statement implies that a characterization of technologies like PETs, including their relation to regulations, is not readily available in many cases, i.e. that this decision of when to use what is not clear cut. In the end, there are many factors that can be causing this, among them the undoubted complexity of such tools.

The elaboration upon this argument is not meant to say that no work has been performed on better understanding PETs and their characterization. Possibly one of the most recent attempts to this regard came in 2015 with the organization of PETs into a taxonomy [55]. Immediately interesting with this work is the definition of PETs as belonging to “a class of technical measures which aim at preserving the privacy of individuals or groups of individuals”. The terminology is intriguing, although the authors make no connection to privacy regulation. Certainly more encompassing is the Handbook of Privacy and Privacy-Enhancing Technologies [56] from 2003, which goes much further to investigate the applicability of PETs in specific use scenarios. This work is also unique in the way that it ties into legal viewpoints of privacy, as well as the EU stance at the time. As it is almost 20 years old, the modern relevance of this work should be investigated. Furthermore, as with [55], the specific relation of PETs to (modern) privacy regulation is not expounded upon. Here, a gap certainly exists.

The discussion of this challenge is deliberately placed in front to serve as an opening discussion for some of the challenges to follow. Promising technologies such as PETs can certainly be included under the umbrella of technical measures for privacy compliance, yet the hows, whens, and whats are still unclear, leading to practical challenges in their widespread implementation.

C2.2: The Factor of Resources

When introducing new privacy-enhancing, or privacy-preserving, technologies to existing systems comes into question, the factor of resources cannot be ignored. By resources can be meant financial or physical resources, i.e. whatever is required to facilitate the adoption of new technologies. Such technologies would ideally be considered a desirable realization of the technical measures required for privacy compliance, yet they certainly do not come for free. This is particularly the case with PETs, which require resources in the form of infrastructure, but also through the education or hiring of experts to oversee the adoption. This notion is confirmed by a recent report on PETs published by the Royal Society [57], which lists among the major limits of these technologies as the requirement for vast computational resources and “specialist skills”.

The decision as to whether certain technologies can be implemented is ultimately a financial one. As one interviewee puts it: “Cost ends up being something you have to really count into. Because if you don’t have the budget for it, you just won’t be able to do it.” (I14-L). Another interesting perspective mentions a specific class of organizations and their ability to approach the technical measures questions, namely that “for a small company it’s [about] resources.” (I12-L). Disregarding the actual desire of an organization to pursue sound technical measures, one sees here that the factor of resources can ultimately lead off the discussion, and in
7. Challenges

some cases, very much influence a decision. In this way, the technical requirement posed by
regulations may be interpreted as an initial strain on organizations of any size, at least from a
purely resource point of view. There are certainly more angles from which one can observe
this dynamic, and some of them will be introduced via other challenges.

Another aspect in the discussion about resources affecting technical measures comes with
the influence on structure. I12-L ties these two concepts together in a succinct way: “We
end up at the resources. And how good is your IT team?”, which juxtaposes the idea of a
“good” IT team, implying one that can implement “good” technical measures, with a sufficient
amount of resources allocated. Specifically from the perspective of a privacy engineer, who
would without a doubt be a proponent for the inclusion of privacy engineers in the process
of privacy compliance, acknowledges that “whether [organizations] have the money to create
a separate privacy engineer ladder is totally different.” (I4-T). Once again, it is exhibited that
a focus on better privacy requires resources, as one might naturally imagine.

The introduction of this challenge may seem self-explanatory or perhaps even obvious, in
the manner that of course the implementation of new technologies will require additional
resources. The true challenge lies in the fact that the discussion around these technologies is
not one that grew organically from within organizations, but rather one that has sprung as a
result of necessary compliance to regulations (and the avoidance of costly fines). Therefore,
the factor of resources is one that not only affects the ability to implement particular measures,
but it also raises questions of incentive, innovation, and equality in compliance demonstration.

C2.3: PETs are Difficult to Communicate

The technology is very complicated… this is a very important issue, that most of the
Privacy-Enhancing Technologies are very hard to use in practice.

Challenge 2.3 certainly feeds off of the potential challenges introduced in C2.1, but it focuses
particularly on the complicated nature of PETs and their ability to be communicated effectively.
Implicit in this is also the ease with which such technologies can be communicated between
the technical and legal sides of privacy compliance, harking back to some challenges discussed
in the first category.

An initial challenge comes with the question of how to include PETs in the discussion
about technical measures, or better said, “how to handle the tools in the best manner, in a
meaningful manner” (I2-T). What exactly is the connection? Without this being properly
defined, the communication of PETs and all their inner workings can become difficult.

Beyond this, it is without a doubt that PETs, particularly the “math” behind them, are not
simple by any means. In short:

...the nature of privacy-enhancing technologies not just because of the newness of
the field, but because of the math and technical complexity behind a couple of
them, they’re not easily communicable. Like, you actually do need a fairly good
baseline knowledge. (I4-T)

The technical complexity alone as expressed here is a good vote of confidence to include this
category of technologies as sound technical measures, but of course this is not sufficient. The
actual manner in which data privacy is protected is arguably more important, particularly in the frame of privacy regulations. Along with the technical baseline required to understand the foundation behind PETs, the mechanisms in place to protect privacy are also not easily communicable. To further exacerbate the challenge, how privacy is defined (in a more technical sense) in the framework of these PETs may or may not be easily understandable, or line up with expected sense as stated in the word of the law.

The main place in which communication becomes challenging is once again in technical-legal interactions. This is particularly true due to the complex nature of PETs. As I2-T puts it:

If you have a bleeding edge topic, and this is with Privacy-Enhancing Technologies, this is often the case, that it takes some time until you are on one page... I would say, it could be that the technical persons are a bit ahead of the legal teams when it comes to Privacy-Enhancing Technologies.

And this is quite understandable, in the same way that legal persons might be more well-equipped to communicate about new regulations. It should also be noted that this statement came on the flip side to the acknowledgement that in many cases where more established technical measures are in play, the technical-legal communication proceeds much more effectively.

The challenge of communication introduced here brings to light some clear needs surrounding the communicability of more advanced technologies like PETs. While the intention of these technical measures are without a doubt well-meant, their current opaqueness somewhat lowers their value to practitioners in the process of privacy compliance. Referring back to a concept previously mentioned, the transition of PETs as a whole from a more “academic” endeavor to clear, actionable technologies represents a major hurdle going forward.

C2.4: No Clear Mapping of PETs

This challenge makes concrete a notion that has been often alluded to in the previous challenges of this category, which is that there is no clear mapping of PETs to regulatory requirements. One may see how this challenge almost comes out of a “chain reaction” from C2.1 and C2.3, i.e. that because there is a lack of proper characterization, PETs are not well communicated, and because of this, there is no clear sense of the role of Privacy-Enhancing Technologies in the field of compliance. In addition, as discussed in C2.1, preliminary work on the characterization of PETs does not generally include strong ties to their applicability to legal requirements. A couple of interviewees provide more insight here.

To ground this challenge in a clearly existing gap, it must be explained as to why such a mapping is needed. This is illustrated by one interviewee, expressed by a need of “case by case reviews of certain technologies to really see if you meet something that is a legal requirement. At least to me sometimes, I would say the mapping is not yet very clear.” (I2-T). One may assume here that the “case by case reviews” would involve individual explorations into particular technologies to investigate their characteristics and relevance to requirements expressed in privacy regulations. The same interviewee goes further to say that technical
measures “that really fall in between legal guarantees will be interesting to see where these will end up and how adoption of these will be fostered.” (I2-T). It can be said that PETs certainly fall into this category. Overall, these insights suggest that the class of Privacy-Enhancing Technologies, however promising they may be in of themselves, currently exist in a sort of gray area for compliance. Indeed, the mapping is not clear.

Viewing this challenge from a legal perspective can also be useful. After all, such a mapping would be just as crucial in the hands of legal support, in order to be able to disseminate proper legal guidance on the usage of technologies such as PETs as technical measures for compliance. Through the interviews, however, it became clear that the concept of PETs in the legal community is not one that is widely known, let alone their mapping to regulations. Without such knowledge, this challenge slowly recedes back to those presented in the C2.1 and C2.3.

Initial research into the pursuit of such a mapping has been fruitful. In [58], the requirements of the GDPR, organized into the explicitly listed data protection properties, are mapped onto different privacy design processes and practices. Such a template for mappings between technology and regulation can most certainly be translated for use with PETs and other complex technologies. In turn, such tools would serve to inform decisions on the appropriate technical measures that should be taken.

The challenge introduced here is definitely a pressing one, as will be explored further in Chapters 8 and 9. To sum it up, in talks about PETs with an interviewee serving as a privacy engineer, the interviewee admits that, “to be honest, I couldn’t understand the legal requirement” (I15-T) with respect to the applicability of PETs. If such a disconnect continues to pervade the technical side of privacy compliance, making a case for PETs as technical measures may continue to be difficult.

C2.5: Lacking Education on PETs

At a minimum, there is this whole academic barrier, not just on understanding what certain technologies mean, but the implications and impact of them. (I9-T)

The final challenge relating specifically to PETs (see C2.8) is one that opens up discussions for later challenges, as well as one major solution concept. Arguably the largest barrier pertaining to the concept of Privacy-Enhancing Technologies is the general lack of knowledge of them, which can be rephrased into the challenge of a lack of education on PETs. Extending beyond “knowledge” itself, the quote leading off this challenge also points to the challenge of understanding the underlying meaning and implications of such technologies. Thus, not only does education become important here, but also awareness.

Before diving into these topics, one may question whether these state-of-the-art Privacy-Enhancing Technologies are even required at all. One interviewee quite clearly puts this question at bay:

If you’re sharing records outside the company, you’re sharing internal data, you’re doing anything with user data, anything with non reset-able machine data, [you
need] to use Privacy-Enhancing Technologies. It’s required. Some companies may not have it. (I4-T)

Of course, this statement comes with a caveat, and this goes back to the “it depends” nature of many of privacy compliance’s questions. Some PETs require specific use cases, and sometimes the data processing in question excludes PETs altogether. Privacy-Enhancing Technologies should not be seen as a cure-all, and there are certainly limitations. These limitations, also discussed in works such as [54], belong to the important characterization of PETs that is very much needed. Nevertheless, the statement from I4-T is certainly grounded in the way that these technologies, despite their potential drawbacks, represent some of the best currently available methods whose goal it is to protect data privacy. Thus, it may be concluded here that while PETs are not strictly required, their intentions are very much aligned with the goals of the privacy regulations in question.

The challenge of proper education traces back firstly to the complex nature of such technologies. Simply, as with any relatively challenging concept, there will exist relatively few experts on the matter. If this is the case, then it can be expected that general knowledge will be lower. And this lack does not preclude some of the forefront technical roles in privacy compliance. As one privacy engineer states with regards to PETs (specifically Homomorphic Encryption in this case), “I’m much more comfortable if I can then turn around and say, hey, with technical specificity, what this is, what it does, what the benefits are, just like any good privacy consultant, but I can’t.” (I4-T). It is argued that when people in such roles are even unsure about the properties of certain PETs, better education is needed.

Even as early as the start of the new millennium, advocates were calling for the more widespread adoption of privacy curriculum within IT and Computer Science programs. For example in [59], a clear lack is noted, not only in university curriculum, but also in coverage of privacy and Privacy-Enhancing Technologies within textbooks and learning material. Although little in the way of continuing research has been conducted here, one can reasonably argue that the state of things has not moved much from what was observed by the authors of this work nearly 20 years ago.

Moving from the concept of education to that of awareness, some interviewees demonstrated a clear focus on the latter. A technical interviewee expressed a frustrating aspect of implementing technical measures for compliance as: “Somehow it is hard when we really make strong arguments to convince them why this technology is very useful for them.” (I15-T). By “them” is meant management in this case. This statement introduces a new recurring theme, that the awareness and acceptance surrounding certain technical measures is almost as important as the technology itself. Several subsequent challenges, both inside and outside of this category, will relate to this theme. A legal interviewee also agrees; in the discussion about PETs, it was expressed that, “I think it would be something that you definitely need a huge awareness piece on.” (I14-L).

With the concepts of education and awareness as the two major pillars of this challenge, one potential shortcoming comes out of one interviewee’s insight. I16-L paints the dynamic where “the laws are evolving very fast and I would say, slowly and surely technology is also running ahead.” (I16-L). This possesses similarities to a sentiment covered in Challenge C1.5.
In addition, it introduces doubt surrounding the merit of education on things such as PETs, when these technologies as well as regulations are evolving so rapidly. To this argument, two points. First, “rapidly” must be put under the microscope – what may be thought of as rapid might not be so much so, pointing to a relative concept. Take the example of Differential Privacy, first introduced in 2006. One may consider the research on this topic to still be in its adolescence, nearly 15 years later, with works on its characterization and applications still regularly appearing.

The second argument comes from the very same interviewee, which is that “continuous learning is a very important aspect of privacy implementation” (I16-L). This was a topic covered in many of the interviews, and one that was often answered in the positive. Therefore, the key to education about quickly evolving topics such as PETs becomes the concept of continuous learning. How this might look, as well as other challenges relating to it, will be covered in various subsequent points.

C2.6: Lack of Technical Literacy

While this concept may be similar to that expressed in C1.4, the distinction must be made. C1.4 describes how a lack of domain-knowledge affects the interactions between people from the different sectors involved in privacy compliance. In contrast, this challenge focuses on how a lack of technical literacy affects the implementation of technical measures. Thus, the technical aspect is highlighted, particularly in relevance to regulations.

On that note, the first difficulty arising out of this challenge comes with a disconnect between data processing practices and what is advisable under regulations. In one example given by I2-T, it was claimed that, “the biggest problem is uncertainty with how well the use of data in machine learning sometimes is in line with the original concept [of regulations].” This topic teeters on the challenge of a lack of technical input in privacy compliance, in the way that regulations might not make clear whether certain practices are “in line”, legally speaking. This example, though, points to another hindrance, that the lacking technical aspect in privacy compliance leads to uncertainty not only in the demonstration of compliance, but also in the practices and/or systems themselves. With a better understanding of these practices, and specifically their relation to regulation, perhaps this uncertainty can be mitigated.

Another topic falling under the umbrella of this challenge relates to the way in which compliance programs are structured. This is motivated by the statement:

There needs to be generally more literacy and appreciation for the fact, like in the computer science, in the legal, in the technologist community, whether it’s academia, industry, wherever, of the fact that privacy is not security. (I4-T)

Such a notion aims at the heart of the technical measures in question, but specifically in their purpose. If one believes the above statement to be true and privacy is not security, then programs aimed at fulfilling technical measures via security measures are missing a crucial aspect of the whole exercise, that is of privacy protection. As such, better literacy on privacy vs. security in a technical sense could be needed (more on this in Challenge Category 4).
7. Challenges

The final idea with regards to technical literacy comes with the relation of technical measures to the willingness to implement them. Namely, the

...tech literacy element of really needing to drive home some of what this tech actually does, you’re more likely to invest in it... Almost like the entire technology behind it, and you feel more comfortable investing in it. (I14-L)

The interesting usage of invest is quite fitting, not in the financial sense, but more relating back to the notion of awareness. In the argument presented here, a higher technical literacy, i.e. higher knowledge of how the technology in question works, leads to a higher willingness to accept and implement said technology. This is certainly an intriguing concept, one that adds to the discussion surrounding the need for better awareness of available technical measures.

The discussion of a lacking technical literacy ends here, with a few examples of its meaning provided above. Surely, this challenge merits further investigation into other aspects of this concept of literacy as it pertains to the process of privacy compliance. As with before, this challenge is by no means aimed at a particular sub-group of the privacy compliance structure. Rather, it strives to emphasize the importance of technical literacy in a process where technical measures have become central.

C2.7: Lack of a Technical Framework

A lot of the technical bedrock doesn’t exist. (I4-T)

This point was without a doubt a major one surfacing in several interviews, particularly from the technical side, but also from legal voices. C2.7 hones in on the lack of an accepted and widely-used technical framework for the implementation of technical measures for privacy compliance. By “framework” is meant a structured technical specification, providing the necessary guidance for technical roles to implement privacy compliant systems. While the concept of a “technical framework” is generally quite broad, the idea refers to an established specification, in the form of documentation or the like, created for the purpose of the uniform systematization of an (industry) process. A prominent example, coming out of the healthcare industry, is the technical frameworks created by IHE International, described as “specific implementations of established standards to achieve effective systems integration, facilitate appropriate sharing of medical information and support optimal patient care” [60].

To start off the discussion of this challenge, it should be noted that the title does not imply the complete lack of any technical framework for privacy compliance. Indeed, some thorough attempts have been published in the literature, such as with the DEFeND Architecture [61] or the more model-based approach of Alshammari and Simpson [62]. Rather, and this is something supported by several interviewees, the perceived lack is derived from the fact that no framework has been uniformly accepted. Moreover, some interviewees were unaware of the existence of any framework at all. This certainly speaks to a clear missing piece. Precisely why existing frameworks have not been widely adopted was not investigated, and this could certainly be the motivation for future research.
The lack of a sound technical framework is quite understandably perceived the greatest in the actual implementation of technical measures for privacy compliance. A legal interviewee acknowledges this, saying there is “a complete lack of a framework as far as I’m aware, for technicians if they build new software, on how to build in privacy automatically.” (I7-L). It is seemingly at this point, when engineers are to design and build a new system, that such a framework would be most beneficial. Referring back to the concept of Privacy by Design, introduced in Chapter 3, such a concept almost hinges upon the availability of a guiding framework. On the technical side, the lack of a framework leads to a certain frustration: “What bothers me most at the moment is that now there are certain requirements and anonymization, for example, and it’s a very vague requirement.” (I2-T). The vagueness mentioned here definitely roots itself in the regulations themselves, as previously discussed. On these grounds, one can begin to make the case for a technical framework, at the very least for guidance and to clear up this “vagueness”.

One may ask, how would such a framework actually help? The answer to this also came via some of the interviewees, and it ultimately rests upon the way in which engineers work. I2-T states directly that “I prefer to really work on a codified text... such that you have really concrete information”, which provides an interesting contrast to the “vagueness” just mentioned. Such a codified text would need to be a specification, but with the necessary legal input to make the process of technical measures implementation grounded in legal requirements. The benefit of a technical framework for technically-minded people (as well as a clear call for those of us in academia), comes with the following:

I think technicians think more in frameworks and how they technically build stuff. And there is no such thing like, such a framework that I can point them to, I can hand some checklists and say, listen, we have to consider those points. There’s not a universal framework... so yes, if you guys at university can come up with something like that, we would definitely be interested. (I7-L)

How exactly this technical framework would be structured is still an open question. One potential insight thereto is provided by I9-T:

I don’t think that there is good tooling that really highlights or connects what is happening in practice with real data flows at scale that’s needed for most organizations to actually sort of show it through privacy compliance.

Important to observe here is, once again, an emphasis on the idea of data flow. In the process of privacy compliance, which at its core aims to protect data, the flow (source, transportation, processing) of such data becomes central. With this insight, therefore, a sound technical framework would without a doubt need to provide a specification on the mapping of data flows. This however, is only one piece to the puzzle, as promoted by [63]. Specifically, the authors here outline five stages that must be considered in the implementation of technical measures for privacy compliance, which ultimately related to this idea of data flow, but break it down into clear stages. Here, another important blueprint is provided for an eventual privacy compliance technical framework.
This particular challenge, certainly among others, provides researchers and industry practitioners alike a clear and present call for continued research. Specifically, the creation of a relevant, useful, and widely acceptable technical framework for the implementation of technical measures is something that could quite possibly alleviate many of the challenges presented in this work. Such an endeavor, however, would require a concentrated, interdisciplinary effort; nevertheless, the prospect of the potential benefits in the end provides a significant motive.

**C2.8 No Incentive for PETs**

*So people who do their homework properly, do not necessarily sadly get rewarded yet.* *(I2-T)*

The challenge presented here, although only mentioned explicitly by one interviewee, is one that plays a significant role in the overall discussion of this second challenge category. In addition, it serves as a clear precursor to one of the predominant challenges in the fourth category (see C4.4). Challenge C2.8 addresses the notion that organizations striving to implement Privacy-Enhancing Technologies are not “rewarded”, in the sense that there is no tangible incentive to do so.

Referring back to some of the first few challenges within this category, it was argued that the implementation of state-of-the-art PETs for privacy compliance presents a relatively large overhead up-front, both in the complexity involved and the resources required. The question becomes whether some kind of clear incentive exists, which would sway the necessary decisions to pursue such technologies despite the overhead. I2-T responds to this succinctly: “There is no big incentive to be the first one to introduce [PETs].”

Now it must also be considered that there does indeed exist some incentives, perhaps not altogether tangible, for the implementation of PETs. I2-T chimes in here with the ultimate incentive, which is “not to get hacked”, putting it simply. Of course, this should be a priority for any organization or entity handling any kind of user-derived data, but one may argue that this incentive falls more into the altruistic category of motives for the implementation of advanced technologies. Additionally, it is certainly not always the case that such technologies, for example PETs, *must* be implemented such that dubious outcomes like data breaches can be avoided. As a result, organizations might be hesitant to “take the leap” towards PETs, when a proper risk assessment demonstrates that this might not be necessary.

In this way, a true incentive for the implementation of PETs, or really any state-of-the-art technical measure, can be perceived as missing. The exact nature of an incentive that would better motivate such technical pursuits is unclear; moreover, it is outside of the author’s knowledge to comment on this. What can be said, however, is that if true, such a challenge can have implications extending beyond the purely technical realm of privacy compliance, as will be explored in the next two challenges, particularly in C2.10.

**C2.9: The Technology is there, the Awareness isn’t**

*All the technical measures are only as good as the people.* *(I11-L)*

---

70
7. Challenges

To introduce this challenge, it is important to note its significance, which is judged not only by the relatively high frequency with which it was discussed in interviews, but also by the clarity of the insights drawn from therein. The introductory quote for Challenge C2.9 provides an excellent summary of what is meant by this challenge, in a quite compact manner. Essentially, in the discussion about technical measures for privacy compliance, one can almost view the literal technical measures as supplementary; that is, the technology for data privacy protection “is there”. The crux of the matter here, though, is the people and organizations behind the technical measures. In other words, no matter how promising (or not) a particular “technical measure” may be becomes irrelevant if the awareness of them is not in existence.

This challenge may be studied from several angles. The first is focused much more on the technology itself. The question of implementation, residing at the core of this thesis, is actually a bit more complex than it may appear on the surface. One insight from a technical perspective on this matter states the following:

I think it’s really easy to implement a technical measure... but to actually make sure that that data is healthy and tracked and like can be produced on a dime... it’s actually expensive and technically complex. (I4-T)

Here, the implementation of technical measures is not the source of the challenge, but rather what comes after. In this way, the step beyond the initial implementation is emphasized, something which arguably may not be reflected in regulation.

Another aspect indicating existing technology, but lacking awareness comes with the perceived level of understanding of such technologies among the people involved with privacy compliance. This insight comes primarily from I14-L, who claims:

There’s a lot of technology out there. It’s a do you know all the types of technology and what it actually does, because a lot of the privacy professionals just don’t have that technical background.

This sentiment almost harks back to the need for a greater technical literacy amongst the privacy professional community, once again pointing the challenge not at the technology, but the awareness around them. I14-L goes on to strengthen this argument, saying that “with some of the tech measures that are there, I think they end up being buzzwords without people understanding what they are.” This is certainly an interesting opinion, one that also speaks to the apparent complexity and opaqueness of many of the options for technical measures out there.

Departing from the actual technical measures themselves, one arrives at possibly the most salient aspect of this challenge, focused on the processes in place surrounding the measures. Perhaps to best introduce this perspective, a quote:

You have to connect data privacy with processes in a company. All the things have to work together... You can do a lot of things with technical measures. But for me, the main part is processes. (I12-L)

This hints at a concept that will become more central in the discussion about organizational factors in the next category. In short, the implementation of technical measures must be
7. Challenges

Ingrained into the processes of an organization, in order for the purpose of these measures to take meaning. To support this idea, one interviewee sees the most challenging aspect of the privacy compliance process as “the issue of raising awareness, both for the teams, so that they would know what issues to kind of identify and what to look at.” (I8-L). This brings the issue back to the people surrounding the technical measures, highlighting a need for higher awareness. And finally, in perhaps the most explicit call for better awareness of the technical measures for privacy compliance:

The most challenging experience is to get access to people’s mind to the fact that it’s not a burden on them, most people see it as a burden on top within the work framework... So for me the most challenging is to get them on the understanding that every single one of us is a subject so every single one of us is affected all the time. (I11-L)

In this light, one could also see this argument as another “altruistic” motive for implementing sound technical measures (referring back to C2.8).

An interesting notion regarding the nature of technical measures is one that also fits under the umbrella of this challenge. Specifically, a couple of interviewees held that technical measures, however these might look, truly play a supplementary, or perhaps complementary, role to the organizational measures for privacy compliance. This sort of “support” role is expressed here:

This is where I sort of scratch my head, a lot of it. So for me, I’ve always been of the opinion, a tool will never give you full compliance unless you actually understand the legislation behind it... for technical measures, it’s to sort of support what you’re already doing, and kind of help lessen that workload. (I14-L)

Surely, a deeper analysis could be conducted as to what is precisely meant in this statement. On the surface, though, two things are emphasized: a need for a strong understanding of legislative requirements for technical measures, and the fact that these technical measures must be met with existing, compatible organizational measures. As part of the organizational measures in question, the technical measures almost certainly come into play: “In the end, you just need a backup of the organizational methods, does everybody know how it’s implemented, how does it work?” (I11-L). As such, the intertwined nature of the two is clearly illustrated. The challenge with this, though, is that a kind of inter-dependency is created, and even with the “best” technical measures, lacking awareness in an organizational structure renders them a moot point.

It should be noted that this challenge was not met with unanimous agreement among the interviewees. In particular, one clear counter-argument comes with: “I just don’t think there are adequate technical measures like, we just don’t have the adequate technology.” (I9-T). This argument, though, does not completely rule out the challenge presented by C2.9. Firstly, the adequacy of technical measures might be different for different organizations; it may be the case for the largest organizations of today conducting massive data processing efforts, there indeed exists no satisfactory measure truly to protect data privacy. Even on this subject,
the meaning of “adequate” must be called into question. What is considered adequate by privacy regulation almost certainly may not be seen the same by a staunch data privacy proponent. Furthermore, this brings up the concept that what true privacy means will differ from person to person. Nevertheless, this interviewee’s stance is not without ground, and it hints to challenges that will appear in Challenge Category 4.

The main points of this challenge can also be found in the literature. In what is illustrated as a unique dynamic, Phillips [64] describes the cycle of legal requirements for privacy, the realization of these laws through technology, and the resulting implications for society at large. A crucial point, however, comes with: “Technical systems of this sort [PETs] are only as socially relevant as they are well incorporated into everyday practice”. This supports the thesis that the existence of sound technical measures is not enough; awareness must also be there, too. The conversation around this matter, as acknowledged by the author, is much more complex – how privacy is defined in legislation (if at all) and how this is perceived by organizations and the consumer will ultimately affect the entire process. This general concept will be picked up again in subsequent challenges, particularly in C3.2 and C4.5.

Concluding the talks of this challenge, one can begin to see an interesting dynamic existing in the field of privacy compliance between the existence of technologies designed for data protection and the awareness surrounding them. In other cases, this awareness might be better interpreted as a “willingness to adopt”. Looking at the silver lining, this challenge presents a clear path for optimization: a focus on building awareness (understanding) of the privacy-enhancing and privacy-preserving technologies of today.

C2.10: Privacy Compliance and Innovation

The last challenge in this category is certainly a divisive one; nevertheless, the fact that multiple interviewees alluded to it merits its inclusion. The accuracy of this challenge with respect to its relevance in practice will be an interesting point to explore in Chapter 8. Essentially, the discussion here is centered around the effect of privacy compliance on the innovation of technology. The challenge, as seen by some interviewees, is that the process of privacy compliance does not necessarily promote innovation. Exactly how this is the case was expressed in a few ways.

An initial way one can interpret this challenge is the pitting of privacy compliance and data-driven innovation against each other. This, coined as the “Privacy-Innovation Conundrum” [65], is certainly an interesting topic to investigate, and it has received some attention. In essence, the conundrum here can be concisely summarized as the “potential for a trade-off between innovation and privacy” [66]. The crux of Challenge C2.10 takes a bit of a different angle, looking not at data-driven innovation per se, but rather at the innovation of technical measures for privacy compliance, e.g. PETs. How this is affected by regulatory requirements presents another interesting, and largely unexplored, area of investigation.

The concept of “state of the art” serves as a basis for this challenge. Taking the GDPR as an example, the requirement for “appropriate” technical measures is soon followed by a call for “due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations” (Opening Clause 78). One could directly assume
that such a requirement would be well-serving to promote the development of advanced technologies for data protection. In practice, this may not be the case. One voice believes that “the state of the art in technical measures is hindering implementation. Just because it sets an unattainable goal.” (I10-LT). The nature of this “unattainable goal” is also hinted at by I7-L: “I always tell the clients it’s not like you have to use state of the art, because that’s so vague, that it can be enforced legally.” What can be extracted from these two statements is the challenge of implementing “state of the art”, when the concept itself is not well-defined by regulations. In turn, incentive to pursue the state of the art may be low, or it may be seen as not even necessary from an enforcement standpoint. In such, a vicious cycle is created.

This introduces an important theory that will only be briefly mentioned here, but one that was adamantly defended in one interview. That is the theory of positivism [67]. Its relevance to the discussion here lies in the manner in which “state of the art” is built into modern regulations, with the hope that it will be reflected in practice. As explained above, this may not entirely be the case. The entrance into a philosophical debate here is undeniable; although highly interesting, it will end here for now, as the author is admittedly ill-equipped to further it.

Continuing the discussion about the challenge at hand, another perspective from which one can view it is from the nature of privacy compliance. Most would agree that the ultimate goal of compliance, taken completely on its own, is to demonstrate legal compliance to relevant regulations. As such, there becomes a point where compliance is “reached”, in the eyes of the law (regulatory authorities, auditors, etc.). In this way, an insight to this matter comes from a privacy engineer: “Compliance actually doesn’t motivate the innovation in the privacy field, telling a company what they do is enough.” (I15-T). This supports the notion that compliance to regulations cannot be the sole motivator for the development of the technologies to do so, since compliance can only push the innovation so far. The ideas presented here will surface again, as it shares ties to other challenges in the next two categories.

The final facet of this challenge concerns the laws in question and the debate surrounding them. The way in which the innovation of technologies for data protection has been inextricably bound together with the requirement for a legal basis could certainly be argued as a hindrance to innovation. This, in turn, might affect the process of privacy compliance negatively. As one interviewee puts it:

Why do we have that legal discussion? Now you have to have a legal basis, even considering the technology’s right - It’s used anyway. So I think the position they’re taking will, in fact, not lead to more privacy, but less privacy, because sometimes some will just not care. (I7-L)

The challenge described here is also reminiscent of that provided in C1.5, pointing to a debate that is too legally-focused, and possibly negligent of the technology itself, and the innovation thereof. One can even take the GDPR as a living example of this, with very little of the text dedicated to a discussion of the technical measures themselves.

A way going forward to address this challenge is unclear. One opinion states that “[if] there is a change in technology, the law should also be changed.” (I16-L). Whether this would directly mitigate the challenge of innovation is also something that is unknown. In the end,
the topic covered here deserves further debate, as it is one that hits at the core of data privacy and data protection.

7.3.3. Summary

This challenge category places a particular focus on the technologies considered as the technical measures for privacy compliance. First, a specific investigation into Privacy-Enhancing Technologies was performed, looking at the challenges introduced by their inherently complex nature, as well as the hindrances this creates for implementation and communication. Next, some perceived gaps in the privacy compliance process were covered, namely a lacking technical literacy and technical framework. Finally, some challenges with respect to technology illuminating larger implications were discussed, with a unifying theme that modern privacy compliance has affected the way in which the relevant technologies are implemented, understood, and innovated.

Looking specifically at the idea of technology, its potential in the pursuit of data privacy and data protection must be emphasized. Taking inspiration from *A Cypherpunk’s Manifesto* [68], a major theme that can be extracted can go something like “privacy through technology, not through legislation” [53]. Although the power of technology can be asserted, one may already understand that this ideal may not be all too realistic in the light of privacy compliance. Nevertheless, the focus on developing, promoting, and educating such technology should not be neglected.

As all of the challenges in the category pertain specifically to the “technical measures” which have been placed under the microscope, they all certainly carry a particular weight. Continuing with a common theme, though, they do not form the complete picture. Even in [68], one learns that privacy through technology cannot be achieved on its own:

> For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one’s fellows in society.

Instead, another important piece to the puzzle is covered in the next challenge category.

Mapping

The mapping for Challenge Category 2 is presented in Figure 7.2. Particularly with this mapping, one can perceive a relatively clear “horizontal” orientation, stemming mainly from technical interviewees, but also a few legal ones. The interpretation of this horizontal orientation can be quite straightforward – those who possess the technical knowledge or literacy will be the ones who introduce the challenges of this category, and who can speak better to the intricacies. As an added note, the technical interviewees were naturally more geared towards technical questions, and as a result the challenges identified in this category originated more from these interviews. Nevertheless, the legal influence to the challenges is also apparent, providing an important perspective to round out the corresponding discussions.
7.4. Organizational Factors

The third challenge category, titled “Organizational Factors”, investigates the way in which the structure, culture, and priorities of a particular organization can affect the implementation of technical measures for privacy compliance. The main hypothesis behind these challenges is one that continues a narrative introduced at several points in the previous two challenge categories: whether or not and to what extent sound technical measures are introduced are largely dependent on the people behind these decisions. One aspect of this argument is obvi-
ous, as technical measures will certainly not implement themselves. Diving deeper, though, why particular decisions are made and what are the underlying factors influencing them, therein lies an interesting point of entry for investigation. In this mindset, the interviewees provided many rich insights into the matter, which shall be covered in the following.

7.4.1. Category Overview

Challenge Category 3 contains eight identified challenges, shown in Table 7.3. It should be noted that for C3.3, this is considered an “implicit challenge”, i.e. one that was not (and cannot) be deduced from a single point of view, but rather one that became apparent from observing the entire field of interviewees. This will be discussed further when the actual challenge is introduced.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Mentions</th>
<th>Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3.1</td>
<td>It is often up to management to make decisions regarding compliance</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>C3.2</td>
<td>Organizational culture or politics have implications on technical measures</td>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>C3.3</td>
<td>Lack of uniformly defined structures and roles</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C3.4</td>
<td>Not enough focus on privacy engineering</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>C3.5</td>
<td>Availability of legal / supervisory support differs by company</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>C3.6</td>
<td>Technical measures are difficult for certain organizations</td>
<td>8</td>
<td>14</td>
</tr>
<tr>
<td>C3.7</td>
<td>Technical measures for privacy compliance is a financial concern</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>C3.8</td>
<td>Technical measures depend on a risk assessment, which can vary</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 7.3.: Challenge Category 3, Organizational Factors

7.4.2. The Challenges

C3.1: The Role of Management

*All technical measures are worth nothing, if they are not implemented right, if there’s not the staff, if the executive level that doesn’t stand behind them, but you need them to understand, this is pretty much the first step, we need the executive level to understand at least on maybe on a one year old basis, why we need that, and then we need them behind that. And then we need the culture to go through to the guys who work with them on a daily basis.* (I11-L)

The first challenge of this category starts “at the top”, at a place perceived by many interviews to hold great importance in the privacy compliance process, and particularly, in the implementation of technical measures. Although people serving in management positions may not be performing the actual implementation, the decisions made at this level directly influence what procedures are put into place. Thus, the challenge exists in this dependence on management, placing a considerable role on the people on this level.
One of the major hurdles encountered on the management level can be described as a lack of awareness for the importance of data privacy, or perhaps even priorities pointed in a different direction. Remaining firstly within the engineering vertical, the managers here play a deciding role: “When the head of IT is aware of the data privacy topic and what’s possible, then you will have a good one. And if not, then not, he must be the one to keep this topic on the list, on the agenda.” (I12-L). And this makes sense, for as possibly one of the most direct supervisors to those who will be doing the actual implementation, such a manager holds considerable sway in the matter.

Another aspect of this challenge extends to the general management level, but sticks with the idea of lacking awareness. One insight points to a possible challenge existing in the management mindset, which will also motivate at least two other challenges in this category:

It’s especially a problem with organizations that historically don’t understand the importance of IT, or that are family owned. Because there you have quite often an age difference in management, like those companies doesn’t have really a way to measure how good they are in terms of information security. For them, it’s just a black box. In their view, it’s just a cost factor. (I7-L)

This concept of “cost factor” is certainly also something that becomes important to the analysis of organizational factors, and it also introduces an interesting juxtaposition that is made clearer here: “That one person [the ‘boss’] will be the one who either goes for compliance issues or just kind of drives the business further.” (I8-L). Of course, this head role does not necessarily need to be one singular person, but the point made here is that some may see the decision to invest resources into privacy compliance as an “either/or” scenario, i.e. one that must come at the sacrifice other business ventures. This point, especially the cost factor, will be looked at more deeply in C3.7.

Management is also integral to the process of interacting with outside support. Specifically in these interactions, the sharing of information seems to be crucial for proper guidance regarding the compliance procedures that should be put into place. One such consultant confirms the challenges occurring sometimes in these exchanges, saying “that is more of a struggle that we see in practice, that we get informed too late. That’s more of a management issue at the end of the day.” (I7-L). The factors of awareness and priority can most certainly also feed into this challenge.

At this point, it may be useful to reinforce the central role of management positions in privacy compliance by sharing a common theme expressed by interviewees. Firstly, I15-T affirms that “privacy compliance is the most important issue for the company or organization. Most of the compliance work is done via management procedures.” This exhibits that even before any work towards privacy compliance can be done, the right procedures must be in place, and this falls upon management. This role can be expressed in more metaphorical terms with: “I would say the C suite employees and that point of contact and HR plays a crucial role to this aspect, because we need someone from the organization to also take the flag ahead and push the whole exercise.” (I16-L). In essence, both thoughts hold the same basis, and that is the dependence upon management decisions and procedures as the
7. Challenges

foundation for privacy compliance in an organization. When this foundation does not exist or is shaky, challenges are bound to exist.

Now the question comes, as usual, of what can be done. Insights from interviewees first and foremost make the distinction from the technical aspect of privacy compliance as it applies to management roles. I15-T sees it as “a big gap... it’s not just technical issues. We cannot just make the privacy protection organization to fire technology. So we need management to have a lot of procedures to be well-defined.” This without a doubt expresses a similar sentiment as the introductory quote: it is not enough simply to promote the technology, when the procedures defined by management are lacking. Specifically as to what is (and is not) needed on the management level to address this challenge, one interviewee provides helpful insight:

They don’t need the legal support, they don’t need the legal knowledge, they just need the right mindset, whether it comes from legal knowledge, or whether it comes from a change of culture within the company, that in my opinion, is sufficient. Because the tech people, they’re not usually our problem. The tech teams, not my team, but the tech teams within the companies, they usually would like to do more... but they need support from the executive level or the culture within the company. (I11-L)

This statement, above all, vouches for a supportive aspect to the role of management, which can be seen as going hand in hand with the role of a “promoter” of sound privacy compliance. Moreover, the idea of organizational culture is brought up, which will nicely segue into the challenge that immediately follows. In the end, many of the decisions regarding compliance, particularly at the “early” stages, are in the hands of those at the management level. It is because of this that awareness and prioritization of data protection matters, and the lack thereof, will greatly influence such decisions. Ultimately, the challenge is summed up as:

Specifically for the management, to kind of get management’s attention to that, this is something that the company must deal with, that’s something where we need to allocate resources, it’s something where we need to put our money into, so that’s always been a challenge. (I8-L)

C3.2: Organizational Culture

We can’t just walk into an organization and say, okay, here’s all the laws, do something. (I3-L)

Challenge C3.2 is centered at a topic seen by many interviewees to be crucial to this thesis, and furthermore, one that the author claims to be of particular importance to this category, and arguably overall. At the core of this challenge is the idea of organizational culture. This idea is something that has received considerable attention in the literature, dating back decades. A deeper look into this is left as an exercise for interested readers. Essentially, organizational culture, although containing many definitions, can be broadly described as “the collection
of values, expectations, and practices that guide and inform the actions of all [members]” [69]. This can certainly be portrayed as a rather abstract concept, but it aims to characterize the defining traits of an organization. For the purposes here, the term *politics* will also be bundled in with *culture*, although admittedly possessing a slightly differing connotation. The relationship to the aims of this thesis lies in the way in which this challenge attempts to synthesize many of the themes brought up by various other challenges. The common ground is that the implementation of technical measures is not performed in a vacuum; rather, the culture surrounding them must be formed and made conducive to the willful and informed undertaking of such processes.

Several interviewees see the placement of privacy compliance as a high priority to be necessary for certain organizations, as well as something that can prove to be a challenge. I11-L begins the discussion:

“The most challenging is to get the executive force on board and maybe implement a culture that understands it and sees privacy compliance, and maybe cybersecurity as one of the pillars that are carrying the value and the voice of a company.”

This builds a bridge between the previous challenge and the one at hand, showing an undeniable link. Most notable here is the inclusion of privacy compliance as a *value* of an organization, not simply a process. As such, the shift towards this kind of an organizational culture, one which *values* the merits and importance of demonstrating compliant systems via sound technical measures, presents a rather weighty task. Simply stated, “the culture change is actually a huge one, to get people on board.” (I14-L).

The challenge also harks back to the idea of priorities, which certainly falls under an organization’s culture. Obviously, data privacy protection is one of a plethora of pursuits with which an organization can devote its time and resources. Ultimately, as one interviewee puts it, “people have different priorities for what systems need to be protected first… it genuinely is prioritization regarding speed and complexity, politics and personal choices.” (I4-T). In this way, some of the challenges from the Technologies category are also brought into consideration, in addition to the role of politics.

Looking at some of the ways in which organizational culture can differ with respect to value placed on compliance measures, one interviewee elaborates on some defining factors:

“The companies that are on board with privacy compliance as values to their company, they usually have enough money, enough resources, enough support from the upper level, and so the culture is there, whereas with those companies where the culture isn’t there. (Ill-L)"

The cost dimension of the whole discussion surfaces once again. Additionally, the interconnect between upper level (management) and organizational culture is illustrated. To provide insight on some more distinguishing factors between differing organizational cultures, I8-L formulates a three-tier hierarchy in terms of organizational approaches to privacy compliance:

“I’ve worked with kind of very strict companies that kind of go by every specific, smallest requirement, kind of this government attitude towards everything… the
second kind of way, or the second group is startups. They just think about going forward and moving forward with the business. And this is something that they usually don’t love thinking about, or discussing, they may be given the basic minimum... then the third group... is a bigger, more mature company, which is done with the initial growth, and now it has to kind of get the house in order and understand what’s going on, get the processes in order.

Once again, the important juxtaposition of “business” with the practice of privacy compliance is shown, tied together with the ideas of growth and maturity.

The lack of a unified, clear organizational culture can lead to problems with the privacy compliance process. One aspect is related to the values discussed above, namely that misaligned values towards privacy compliance can be detrimental. An interview shares a personal experience, where “it got into that turf warfare sort of thing… that goes with willingness to accept or ignore privacy risk and privacy compliance risk because of internal organizational development, or organizational politics.” (I9-T). Now, challenges must not always take such form, and another interviewee sheds light on how the literal structuring of an organization, particularly the proximity and inter-availability of the different parties involved, can affect the process:

In organizations, in management structures, this [collaboration between departments] has to be reflected. Because if they’re just placed too far apart, if the legal department or the head of legal or whatever, in the IT department, maybe even outsourced IT department, and then there’s maybe the chief information security officer somewhere, if that is if the organizational structure doesn’t even allow them to work together, then there’s really trouble already. (I5-LT)

Particularly relevant to the idea expressed here is the need for all involved stakeholders to be held equally accountable for their role in the privacy compliance process. To this, one particular frustration becomes apparent:

Some stakeholders and employees want to be compliant, but stakeholders feel like that’s not relevant to them, they feel that they are not dealing it with, and ultimately it becomes an hindrance altogether. (I16-L)

This could be traced back to a missing piece in the organizational culture that prevents a mutual understanding between different stakeholders within an organization (or even external ones too).

The influence of organizational culture of compliance practices has also been studied in the literature. Specifically pertaining to security compliance, the authors of [70] claim that “the problem is not so much with security technology as it is with the lack of security awareness”. This can logically be extended to privacy. Additionally, the lack of awareness does not just fall within an organization, but can be extended to include the users as well.

A brief excursion is taken from the internal culture of an organization to address the literal definition of culture as it pertains to privacy compliance. This takes root in a field of study that has attracted much research attention, such as in [71] or [72], which aims to investigate
7. Challenges

the (socio-)cultural differences when it comes to views on information and data privacy. Even predating this is the idea that privacy in general is perceived differently across the globe. How this pertains to the topic at hand is that the organizations in question, whether it be management, the employees, the customer base, or other stakeholders, range from an incredible variety of cultures and regions. One can only reasonably assume that the emphasis placed on privacy compliance, and the technical measures for it, will also differ by just as much. One concrete challenge brought up in an interview hits right at this notion: “Now, a multinational [organization] that has operations around the globe, how do they deal with [compliance]?” Even in the case of uni-national organizations, one may question how entities from different continents, for example, may operate in the face of far-reaching legislation such as the GDPR. As a more facetious, but telling, comment to this matter, I12-L says, “I don’t think that America has any data privacy in any way!” Of course, this singles out a particular nation, but surprisingly, the topic of the “American” versus “European” approach to privacy compliance came up in multiple interviews.

It is important to tie this discussion back to the topic at hand, that is the challenges to the implementation of technical measures for privacy compliance. The decision to implement (sound) technical measures into the systems and processes in place must be an active one made within an organization. If the value system within an organization places high priority on data protection, then doing so becomes a matter of choosing the appropriate technology (which may also be somewhat challenging) and performing the implementation. The true challenge described here, though, comes as a result of when organizational culture does not include this emphasis on data privacy – in this case, technical measures may not come into question if privacy compliance is not held as important. The caveat here comes with the idea that privacy compliance is not binary, meaning that it must not be the case that organizational culture either allows for or prohibits proper compliance programs. It is argued, however, that such culture has an effect on the degree to which compliance is pursued. The discussion continues on in some of the subsequent challenges of this category.

C3.3: Lack of Uniform Structures and Roles

As introduced in the Category Overview, C3.3 is unique because it is the only challenge defined as “implicit”, meaning one that has been created as a result of an analysis of the interview findings as a whole, and not one that was explicitly mentioned. Such a challenge could not even be reasonably expected from a single interviewee, as it possesses more of a comparative nature amongst organizations and their privacy compliance structures. The argument here is that a lack of uniformly defined structure and roles as they pertain to privacy compliance can create challenges for the field moving forward.

Observing firstly the structure aspect of the challenge, one can confidently say that how the process is carried out in different organizations is not “down to a science”. Chapter 6 presents a generalized view of the structure, pieced together from the insights of all of the interviewees. It is true that within the structure, some roles (particularly the DPO) are in place for the large majority of cases. Apart from this, differences certainly begin to show. The number of roles from the technical side involved in privacy compliance can highly differ based upon the
organization size and purpose. The inclusion of legal support, whether it be internal counsel, external counsel, or external consultants was also covered in Chapter 6. The influence of management roles was heavily emphasized in some interviews, but less so in others. Even the existence of privacy engineers seems to be biased towards larger technical organizations, a challenge that will be introduced next. Finally, referring back to the previous challenge, the stakeholders that should be included in the process are not always well-defined.

In a similar manner, the roles and responsibilities for the privacy compliance process are also a bit murky. A prominent example of this was seen in the discussion of liability in Chapter 6. Other indicators can be seen for example in the wide range of responsibilities falling under the title of Privacy Engineer. In separate interviews, people serving in this one role held duties ranging from audits to consultation to technology development. While this certainly speaks to the dynamism of such a role, it presents a challenge for pinpointing how this particular role fits in the whole picture. Other examples, remaining on the technical side, show roles hailing from many different departments converging on this process of compliance, whether it be from cybersecurity, product design, software engineering, etc.

One cannot assume, at least for the present, that all organizations across the globe, regardless of size, scope, location, or purpose, will share the exact same privacy compliance structure. This is just not reasonable. The example of a Data Protection Officer as a defined role, though, provides an excellent template for how regulations can guide the process, such that a more uniform structure can be reached across the board.

It is argued here that a better comparability between the privacy compliance processes of organizations, especially horizontally with a sector, would not only provide more structure and direction to the demonstration of compliance, but could also lead to boosted transparency and accountability. A well-placed emphasis on such a defined structure could also aid in increased awareness and importance placed on the practice. All of this, one may imagine, would trickle down to the implementation of technical measures. As mentioned, a particular area with a perceived need for improvement is covered next.

**C3.4: Lacking Focus on Privacy Engineering**

The challenge presented here comes particularly from the opinions of two privacy engineers themselves, stating that a larger emphasis needs to be placed on the practice of Privacy Engineering in the process of privacy compliance.

Referring back to the discussion held in Challenge Category 1 about the gap in the technical and legal mindsets, I4-T believes one particular solution could be helpful. In continuance of the discussion of the fundamental nature of “the gap”, I4-T says, “...that gap is okay. And that’s why the world should have more privacy engineers at more companies.” The quote places the role of Privacy Engineer directly in the center of this gap, confirming in a way the denotation of the role as a “Go-Between”.

The role as a Go-Between goes even further. In [73], the authors address a number of potential benefits from the emerging field of Privacy Engineering, among them the way in which it “responds to this gap between research and practice”. Specifically, they outline how “privacy research in computer science has produced a rich array of privacy solutions; however,
the integration of these into everyday engineering practice has been slow”. This very much comes in agreement with some of the challenges discussed in the previous category. As such, privacy engineers have their work cut out for them.

Another privacy engineer provides insight into how this role plays a necessary part, as well as a challenge introduced therein. Specifically, a wish is expressed for a “very good privacy engineering procedure which could help the developer to do the right thing. So we got to get the education to them and we can provide some technology, but sometimes we are just challenging their time and their capabilities.” (I15-T). Firstly, the guiding nature of the privacy engineering role is emphasized. In privacy compliance, and particularly with regards to technical measures, a privacy engineer can provide crucial direction to the developers performing the actual implementation, since as Go-Betweens, the privacy engineers also possess, to a degree, the relevant legal knowledge needed to assist in technical matters. The challenge comes when education is missing somewhere along the line, or if privacy engineering procedures are lacking in general.

Yet another point to this challenge relates back to C3.3, specifically in the way that an imbalance in the privacy engineering field is perceived. An insight comes from I4-T:

I think distributing privacy engineering talent across the community, like more companies of large and mid size, trying to set up their own functions, is also important... if only five of those companies have privacy engineering teams, that’s a huge issue.

Under the surface of this statement is the acknowledgement that while many larger tech companies may be pouring resources and focus into privacy engineering, this is not uniformly distributed by any means. As such, the concept of privacy engineering may be foreign to small- to mid-sized entities, whether their primary focus is technical or not.

The proponents of privacy engineering included here would certainly promote its more widespread practice and acceptance in the process of privacy compliance. In addition, this could optimize some of the compliance programs in place, playing a crucial role at the intersection of technical and legal mindsets and representing a technical counterpart to the DPO. Referring back to themes raised in previous challenges, the implementation of technical measures cannot be done in a vacuum, i.e. the legal aspect should not be ignored. In other words, “Purely technical approaches might prove insufficient for aligning nuanced legal policies with engineering artifacts” [73]. In response to this challenge, the authors here as well as some of the interviewees would certainly point to the widespread adoption of privacy engineering as a clear solution. The feasibility of such an endeavor, as well as the appropriateness of this particular across the industry, remains to be investigated.

C3.5: Availability of Legal and Supervisory Support

C3.5 roots itself in potential challenges raised by interviewees, but also some needs when it comes to sources of support. The integral role of legal guidance was discussed both in Chapter 6 as well as Challenge Category 1, so it will not be reiterated here. Within this challenge also becomes apparent the supportive role of supervisory and/or regulatory authorities. The
availability of both types of support can significantly affect the privacy compliance programs of organizations. A particular gap comes to light concerning the overall availability of such authorities, something which seemingly has not been adequately researched.

The question of legal availability certainly becomes an organizational factor and is determinant on the processes in place. One technical interviewee sees that privacy compliance “arguably should not require consistent communication on a daily basis [with legal], but it does require processes to have been built out. So depending upon where an organization is, in that process will determine more or less where I think I need more interaction with legal.” (I9-T). The main point here is the “processes” that have been built in order to make legal support available for the technical leads of privacy compliance. Regardless of how often legal support is sought, the lack of such processes can be detrimental to engineers in charge of the implementation of technical measures.

The point of support from supervisory authorities is one that affects not just the technical side, but also the legal. This is made evident via a legal frustration: “So one of the challenges we’re struggling with is getting precise answers from the data protection authorities” (I7-T). As discussed in Chapter 3, there are indeed some very helpful material disseminated by authorities to try to guide the process, but the statement above hints that this may not be enough. Especially in light of the technical measures (and many of the arguments from the Technologies category), it may be the case the these authorities are currently unable to provide guidance in some technical areas. Here, an interplay between this challenge and some purely technical challenges is created.

A desire for more supervisory support is made clearer in the discussion of Chapter 9, where this is portrayed as a major area in need of work for the future of privacy compliance. One can begin to understand this – without proper support from legal counsel and data protection authorities, the process of privacy compliance can quickly become an individual, interpretive endeavor.

C3.6: "It Depends"

There are no kind of cases when you could adopt a copy-paste solution for various entities, because it will always be different, there will always be different data elements, different sensitivity of the data, different infrastructures in place. (I8-L)

The challenge presented here is perhaps one that is self-evident, but its effects on technical measures should be elucidated. Ultimately, the challenge rests on the wide diversity of what is referred to as “the industry”, and how the definition of technical measures might waver from organization to organization. In short, it definitely “depends on the data you’re processing” (I2-T), but there are also other aspects to consider that were brought to light in the interviews.

The first facet that will be analyzed is this idea that “technical measures differ from organization to organization” (I16-L). This not only makes the job complex for those implementing technical measures, but also for those providing guidance or consultation on which measures are appropriate for a specific situation. Again, there are no “copy-paste solutions”. Seen from a technical perspective, “No privacy engineer is going to get tactically specific guidance”
(I4-T) on technical measures, specifically with the more technical details. I2-T adds on to this sentiment by saying “I was really sad by the amount of “it depends” answers” (I2-T), reminiscing on initial impressions of the privacy compliance process. One may even trace this challenge back to the regulations themselves and their intended broadness:

You have to have state of the art IT systems. And depending on the sector, that is quite vague, I would say, what are the specific standards that I have to meet. (I7-L)

Here, call for sector-specific guidelines is clearly expressed. Indeed, many of the answers to questions on technical measures may be “it depends”. Other factors come into play.

When considering technical measures, the type of systems to which they are applied will most certainly also differ from organization to organization. One of the clearest challenges to this coming out of the interviews looks at the backwards compatibility of regulations, i.e. how well they are defined for all types of data processing methods or systems, new or old. I1-T, in talks about working on systems as old as several decades, admits “it’s still really a struggle, the industry is trying to invent some backwards compatibility for these requirements, for these laws.” A similar idea is also clearly echoed in another statement:

But one mustn’t forget that we maintain products that sometimes are over 20 years already out in the market. And when they were released to the market, there was no such [privacy] requirement. (I2-T)

A major factor is introduced here, especially for organizations managing “old code”, as I4-T puts it. Regulations such as GDPR demand state of the art technical measures, but how this can be reconciled with not so state of the art systems is an open question. In this way, a very interesting sub-challenge is created.

Perhaps the most mentioned aspect of this challenge comes with the concept of the size of an organization. This can refer to literal size, number of employees, resources available, global reach, and so on. In general, the discussion here revolved around the comparison of “small” vs “large” organizations and their approach towards technical measures. It is seen that the implementation of technical measures may be more difficult for smaller entities. One opinion states: “Small companies… maybe they even don’t have the capacity to look at privacy protection. So it’s very hard to achieve, for a big company it’s easier.” (I15-T), and this is directly reflected in another statement, this time from a legal perspective: “I think the GDPR is too over-engineered for a lot of companies, the small ones. For small ones, it’s really a big effort to fulfill the things there.” (I12-L). Here, the GDPR can certainly be seen as a proxy for modern data privacy regulations as a whole.

In the discussion here, it is important to point out that the distinction between “small” versus “large” organizations and the challenges they face is not so cut and dry as it may seem. In short, this is validated when I12-L adds a caveat to the statement made above: “It’s difficult because size doesn’t matter” (in some cases). A perfect example comes from this very interviewee, who explains the complexity of such a distinction between a multi-hundred employee cleaning service and a micro-sized FinTech startup processing lots of user data. Here, clearly size in the literal sense would not be the most reasonable way to measure appropriateness or necessity of sound technical measures for data privacy protection.
The complexity in this distinction also enters another dimension with the idea of awareness and resources. I4-T leads the discussion:

I would say just generally speaking, that [large tech companies] are the most technically equipped, not just to stay ahead of regulations, but they have the tooling teams and infrastructure to be well ahead of where regulations are, the question of where they are, or who doesn’t fall into the gap between, there are still mid and large sized companies who don’t even know what they have in their logs cluster.

This idea of being “technically equipped” to be able to tackle the requirements imposed by these technical measures is a big one. Some of the larger tech giants of today are mentioned to emphasize that when the resources and technical backbone are readily available, approaching the implementation of technical measures is much better fostered.

In summary of this multi-faceted challenge, the central theme is that the “it-depends-ness” (for the lack of a better term) inherent with the field of privacy compliance can be a source of uneasiness, or rather unevenness, leading to challenges in forming a clear picture of what technical measures entail. For one, it certainly “depends on the amount of people working for the company, from the stage of business, and kind of all of these factors come into play” (I8-L). As to what can be done to address this, I8-L continues on: “It also takes a lot of resources and a lot of energy. So I think that there should be some kind of additional measures or additional mechanisms that could assist companies in this.” With this and the insights discussed here, one hopefully begins to see a clear path for going forward, and arguably it starts in the regulation. Perhaps part of that is also the need for a guiding technical framework that fully acknowledges and adapts for the variability existing amongst the vast diversity of entities in play.

C3.7: Technical Measures as a Financial Concern

Cost ends up being something you have to really count into. Because if you don’t have the budget for it, you just won’t be able to do it. (I14-L)

Privacy is a not a showstopper for business. On the other hand, it’s actually something that helps most businesses. (I11-L)

In this challenge, the discussion circles back to the idea of technical measures for privacy compliance as a cost factor. Here, though, the investigation broadens the scope of this financial concern, looking both at pre- and post-factors revolving around the resources required to pursue these technical measures. In this light, technical measures end up becoming a financial concern in many steps along the way towards compliance. Thus, the analysis is divided into three categories.

When discussing with interviewees some of the major changes seen in the field of privacy compliance in recent years, a frequent type of response centered on the financial concern introduced by the new threat of fines. This new development is even described by a “culture change” by one interviewee:
Since the fines went up, the culture changed. Before that, there was the regulations they were there, they were not much different to now, but no one was fined, or the fines were so little, no one really cared about them. But now the fines are high. So the privacy compliance increased and got more power. (I11-L)

It is interesting to observe that the fear of fines served as a stark motivator for the implementation of technical measures, and one cannot help also to acknowledge the positive aspect here. Particularly with technical measures, one technical interviewee illustrates the shift in mindset towards these technologies:

I would say what they achieved is they opened up a business case for security, because in the past security and privacy departments, from my point of view, were often struggling to get investments... And now with the potential fines that can occur to you, then it’s a lot easier to receive investments. (I2-T)

The motivation to invest in sound technical measures does not even need to rest purely on the threat of fines. Rather, in the modern digital world, the possibilities of breaches is also very much on people’s minds: “The technical measures being implemented is something everybody wants because most companies are afraid. They don’t want to be part of a cyber attack. Because that really costs money.” (I11-L). In essence, a predominantly financial matter can be pinpointed as a strong motivator bringing many people to the table of privacy compliance, and fueling the discussion about proper technical measures. Whether this aspect can be more as a challenge or benefit is up to debate, but the financial influence cannot be denied.

The central aspect, one that pertains the closest to the technical measures themselves, is the availability of resources and budgeting for the implementation of technical measures. This concept has been brought up before and will be reinforced here. The main dynamic here is the balance between “running the business” and at the same time, investing resources to ensure this is done in a compliant manner. I8-L paints a clear picture to this point:

A company has already built their own internal systems, and the infrastructure and so on, and then some DPO comes in and says that now we need to do that, that and that... the main point is resources, financial resources.

This is a tough situation because it certainly falls under the DPO’s job to provide guidance on the appropriate measures that should be taken, but this can seemingly sometimes be at odds with an organization’s available resources. Another statement in support of this comes with: “We end up at the resources. And how good is your IT team?” (I12-L), placing a particular focus on the resources required to maintain a strong technical team. One is reminded of I4-T’s acknowledgment that while privacy engineering should become more universal, whether or not the resources are there to implement such a structure can be uncertain. Unfortunately, this leads one to believe that the ability to implement technical measures is largely dependent on financial capabilities, which could be particularly challenging in the cases where the “culture” is there, but the money isn’t.
7. Challenges

The third and final perspective from which one can steer this discussion focuses on the notion that “it’s something that can change the price or the value of the company” (I8-L), i.e. post technical measures implementation. This is something mentioned by several interviewees, specifically from the legal side. The main argument here is that the ability to demonstrate proper privacy compliance increases value, in the way that it exhibits sound data processing practices. This, in turn, begins a positive cycle, as well explained in the following:

...privacy compliance makes your business in my opinion, more valuable. And also the data that you use is more valuable, because you got the data in a compliant way and now that the data in your company, you have to safeguard with all the technical and organizational measures, you have to take care of it. (I11-L)

This interviewee argues that the responsible collection and processing of data will almost necessitate the proper technical measures to protect it. If true, this attitude towards approaching technical measures can certainly also lead to “commercial benefit”, as claimed here:

...if you think about it, if you give data subjects more rights, and you’ll seem to be really strong on the privacy front, that might be your commercial benefit, because they’ll see you as the strong one... it could be the differential factor. (I14-L)

One may question, though, where the challenge lies. This is also something addressed in the interviews, and the answer is quite clear and insightful. It revolves around the “fear” (an often-appearing term) around the privacy compliance process, which can largely take root because of the financial concerns discussed. If the truly (positive) value behind implementing technical measures, whether it be normative or purely business, cannot be perceived, then the demeanor towards addressing data privacy will not be positive. Surely, the lurking possibility of being fined and the measures required to avoid these upfront, “negative” costs exist, but it is fundamental to see that the return on investment is not simply to “break even”, but rather to distinguish oneself and boost value (and arguably integrity!). The discussion of technical measures as a financial concern is therefore a complex one, certainly with two sides to the same coin.

C3.8: Technical Measures and Risk Assessments

The final challenge in the category covering organization factors looks at the way in which the implementation of technical measures depends on a risk assessment that is conducted. A brief insight into how this process may be structured was provided in Chapter 6, in the discussion around documentation. The challenge here comes with the subjective nature of a risk assessment, as well as when such an assessment is not performed at all.

It may be helpful at first the examine the nature of a “risk assessment”. This is addressed in one interview:

If you look at the risk management methodology, the goal is not to minimize all the risks, but the frequency or probability of an attack and look at which was the most important. (I15-T)
Thus, notions such as prioritization come into play, suggesting that the assessment can be influenced by other factors. In this process of identification, analysis, and evaluation of the privacy risks in question, there are bound to be subjective judgments made. On one hand, the risk assessment carried out for privacy compliance can be seen as the “common denominator” [74], allowing all organizations to evaluate their potential privacy risks and the strength of technical safeguards in place. This common denominator, though, can be viewed from another angle, that is where the commonalities end.

On this note, the analysis of risk assessments for privacy compliance very much fall into the “it depends” category, referring back to C3.6. A legal interview also hints at this, saying “it always goes with the data, they look at the data that you process, then I kind of, I try to assess the risk for the individual.” (I11-L). Again, one must be careful not to ground the challenge in this aspect, as the variability in data processing is a given, and will presumably always be so.

The discussion, therefore, moves to the importance of conducting risk assessments within an organization. Essentially, “you can’t understand what kind of measures you need to take if you haven’t carried out any assessments of your own.” (I8-L). The challenge in doing this ties together many of the challenges already discussed and those to come. Fruitful communication between technical and legal experts, informed knowledge about the technologies at hand, and proper organizational processes in place can all contribute to good risk assessments, both in the identification of data privacy risks, as well as implementation of the proper technical measures.

Organizations ignoring or not conducting these risk assessments can be hindering the privacy compliance process. As I8-L sees it, “on the basis of all of that, the baseline is a company’s own risk assessment, which is something that not a lot of companies do, or that companies have.” The need for stricter requirements to do so or better guidelines on how to conduct these assessments can be argued for, and the current state regarding this will be discussed in Chapter 9.

7.4.3. Summary

The collection of challenges presented under this third category are unified in the proposition that organizational factors possess a crucial role in the implementation of technical measures for privacy compliance. Many of these challenges can occur in-house: the role of management, organizational culture, definition and prioritization of roles, availability of external support, and risk management procedures are all factors distinct from, but ultimately influencing the decision regarding technical measures. Other challenges can certainly be observed from a more comparative standpoint, such as the variability of data privacy requirements for different organizations or the financial concerns in play. These challenges, and surely the ones yet to be uncovered in this category, present an insightful and potentially often-overlooked perspective on privacy compliance, one which may merit considerable future work.
7. Challenges

Mapping

The mapping for Challenge Category 3 is presented in Figure 7.3. Note that for one particular mapping (I11-L, C3.7), four occurrences were enumerated, so this is now presented as the maximum (as well as for the next mapping).

Figure 7.3.: Challenge Category 3 Mapping

Figure 7.3 presents an interesting case, almost in contrast to that shown by Figure 7.2. Although not definitive, this challenge category is rather “vertically” oriented, with particular
challenges receiving considerable attention. In addition, one may argue that the legal influence is dominant in this category, with many of the mentions and occurrences originating from legal voices. An interesting hypothesis can be conjured at this point, that the organizational factors surrounding privacy compliance are of special importance to the legal roles involved, and moreover, that the challenges encountered here can be perceived the most by legal persons. This makes sense, in the way that many times, legal roles can exist much more in the organizational sphere, rather than that of the engineering vertical. Even so, the technical input in this category must not be ignored, and this indicates the inevitable influence of organizational factors even on the technical side of privacy compliance. Either way, the analysis of Figure 7.3 can be quite fruitful.

### 7.5. General

The final challenge category is one that is hopefully self-explanatory from the title, and it is one that aims to tackle some of the “broader” challenges of privacy compliance, which certainly will place some of the discussions more in the abstract realm, rather than pertaining to technology or organizations, for example. It is for this reason that many of the challenges truly tangent on the topic of technical measures, and they can surely also be connected to other areas of privacy compliance or data privacy in general. Nevertheless, the introduction of these general challenges will always be done in the scope of their impact of the implementation of technical measures. In this way, many of the forthcoming challenges provoked interesting conversations and subsequent insights, as their ideas connect this specific topic at hand to a larger picture. Furthermore, they represent predominantly unexplored frontiers in regards to the research landscape, and as a result, largely take the form of introductory arguments.

#### 7.5.1. Category Overview

Challenge Category 4 contains seven identified challenges, presented in Table 7.4.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Mentions</th>
<th>Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>C4.1</td>
<td>The amount of regulation (and “settings”) makes technical measures complicated</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>C4.2</td>
<td>Bureaucracy is a huge challenge</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>C4.3</td>
<td>Industrialization of privacy</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>C4.4</td>
<td>“Bare minimum” technical measures / inequality</td>
<td>9</td>
<td>16</td>
</tr>
<tr>
<td>C4.5</td>
<td>Privacy itself is difficult to understand or define</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>C4.6</td>
<td>Privacy is often conflated with data protection / security</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>C4.7</td>
<td>The true meaning of privacy has been lost in modern privacy compliance</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

Table 7.4.: Challenge Category 4, General
7. Challenges

7.5.2. The Challenges

C4.1: Many Regulations and Settings

There’s gonna be something else that will come along that will capture people’s imaginations that way. Now, GDPR is the thing. (I3-L)

The motivation for the identification of this challenge came out of an important lesson learned early in the interviews. It can be somewhat convenient to see the GDPR as the data protection regulation, and this impression may have already been gained up to this point in the work. The true fact, though, that must be kept in mind, comes in direct relation to the introductory quote above:

GDPR is just one of hundreds of laws that impact what information you can collect you being a corporation, what information you can collect, how you can collect it, what kinds of representations you have to make to individuals. (I3-L)

On top of this, there are countless “settings” in which regulations must be considered and enforced, a discussion started by Challenge C3.6. Combined together, these ideas can sometimes be overwhelming, and its implications when it boils down to the implementation of technical measures is an interesting point of study.

At a high level, the sheer amount of regulation existing in the wild can be a cause for challenges. According to an active tracking performed by the United Nations Center for Trade and Development [75], currently 67% of the world’s nations have adopted data protection and privacy legislation, with an additional 10% in the drafting stage. The is quite incredible when one thinks about it – certainly much larger than simply just the GDPR. And this statistic does not even cover the amount of regulation within nations. This topic of many regulations was certainly addressed in the interviews, for example where one interviewee sees a challenge with it:

It might be even just the global harmonization piece, if you come out with more contradicting pieces, it ends up costing more for the compliance because you’re having to do different pieces just to come by in different jurisdictions. (I14-L)

In relation to the amount of regulations, another legal voice gives one example of the consequences of the intricate web one must navigate, saying “A lot of lawyers create tables and charts and things like that. And to me, it’s just after all this time, it’s just too much.” (I3-L).

The effects of the state of regulations on the privacy compliance process are pretty clear. Looking at the technical side, i.e. those that must build compliant systems, determining what might be relevant requirements could be a frustrating process:

If every privacy engineer [any large tech corporation], so anybody in the privacy engineering community read the law, they’d be too confused to build anything... It’s a beast. (I4-T)
7. Challenges

Determining what measures should be put into place can ultimately lead to less data protection, as supported in this statement: “If you don’t know what those measures are inherently with, like no matter what, you can’t really have consent, regardless, and you can’t have that privacy.” (I9-T). This certainly also refers back to the challenge of interpretation, and moreover, who is the authority here.

Another challenge arising is one that concerns all parties of privacy compliance, and it certainly incorporates the factor of the many “settings” in play. Ultimately, this adds to the idea that the process of privacy compliance can largely be a “gray area”. One interviewee leads the discussion:

 The problem on the legal as well as the technical side is that there is no template there. No clear, ideal 100% compliance example where you could just say, okay, we’re going to do exactly that. And we’re going to be fine. Because it’s so diverse that I think even 10 years from now, even if we had 100,000 customers, we wouldn’t have seen every possible setting. (I5-LT)

This notion of 100% compliance is an interesting one, making a clear case that the demonstration of compliance is hard to measure, and it exists on a scale. The idea here is also voiced by a technical interviewee, rather succinctly: “Realistically, I don’t think anyone can accurately say whether they’re fully in compliance with the law.” (I9-T). And herein lies the challenge, which can certainly be aggravated by the sea of regulations in existence and the uncertainty of what applies where, in what way.

Yet another aspect to this is one that reintroduces an idea also previously discussed, and that is the perception of privacy. Specifically, “compliance is also a very complicated issue because privacy laws are different in different countries and also ethics question because different countries have different perceptions” (I15-T). Since cultural perceptions of data privacy can differ significantly, it is reasonable to believe that these differences are ingrained into the regulations themselves.

The discussion here, although interesting, presents arguably one of the toughest ways forward. In particular, the challenge created by the amount of regulations and settings is not one that can be easily reconciled. One interviewee paints the ideal picture of a “harmonization with data protection, it would be easier if everyone just kind of took the same blueprint and stuck to it.” (I14-L). At the same time, the idea of a unifying “blueprint” sparks an utmost intriguing, albeit idealistic and challenging, concept for the future of privacy compliance.

C4.2: Bureaucracy

It’s only about bureaucracy. It’s not about privacy, it’s about bureaucracy. (I10-LT)

Challenge C4.2 presents a view that needs not too much discussion, and it is certainly one bound to be particularly divisive. Essentially, it comprises of the opinion that the process of privacy compliance involves a significant amount of bureaucracy, which can sometime serve as a detriment to data and privacy protection. The concept of bureaucracy is without a
doubt in general quite difficult to quantify or even reasonably observe, yet nevertheless, some interesting points were brought up to speak to the possible implications to the topic at hand.

One would be hard-pressed to argue against the fact that the rising necessity of privacy compliance has introduced some degree of bureaucracy added to an organization’s typical processes. The time and resources involved, interactions that must take place, and documentation to be completed all can certainly add to it. Indeed, one interview admits that you “can’t escape some level of bureaucracy if you want to be compliant” (I8-L). A perfectly valid counter-argument would be that any compliance process would share similar properties in this regard, that it is simply inherent.

Taking one step further, the particular case of privacy compliance leads some to believe that bureaucracy is especially rampant, even to the point of being a true challenge. One particular interview finds, “It’s amazing how bureaucratic it can get”, even naming the process a “bureaucratic monster” (I10-LT). Obviously, some hyperbole is in play here, but the point is made clear; furthermore, the claim is backed by a more detailed explanation, which transitions well into the next point:

Material change is hard. It costs money. It’s complex, you have to change technologies, you have to change databases, you have to occupy lots of programmers to make it happen. While passing laws… (I10-LT)

An important juxtaposition is made here, one that almost pits the “material change” afforded by true privacy protection against what is required by the law. In this interviewee’s opinion, a certain dynamic has been set into motion where the passing of regulation has almost become a “bureaucratic response” to keep up with the development of technologies. A challenge is illustrated here, one that almost represents the antithesis of what modern privacy regulation should be in its relation to the technical measures available.

The feeling that bureaucracy affects an organization can extend beyond just the implementation of technical measures, but also the process of innovation itself (recall C2.10). This is hinted at when I14-L states: “There’s a bit of a talk about kind of taking away some of that red tape and making it a bit easier for businesses to innovate.” In this way, one learns that some might even see privacy compliance and all that it entails as a direct competitor to innovation. Whether or not this is actually true is one thing, but the fact that such a perception exists calls for deeper investigation (and possible change).

As a useful parallel to bolster this discussion, one can refer to the work titled Technology, Bureaucracy, and Common Sense [76]. In this editorial for the work A Great Opportunity for Innovation in Health, the nature of regulations is claimed to be premised on “common sense”, but the balance between this well-intended bureaucracy and the actual underlying notion to which regulation aims to promote is a fine one. Specifically in this case, the juxtaposition of minimum compliance for quality healthcare and maximum fostering and motivation of stakeholders to create (innovate) better healthcare is made. A direct analogy can be drawn to the implementation of technical measures for privacy compliance, alongside the parallel innovation of better data protection technologies. In the end, this certainly presents an interesting and thought-provoking spin on the topic of bureaucracy.
7. Challenges

The author acknowledges at this point that the challenge introduced here can be a touchy subject. At its very core, some of the internal mechanisms of the privacy compliance structure must be at least somewhat “bureaucratic” to get the job done. The question of whether some of this bureaucracy, if at all existing, can be optimized is a good avenue for future work. Even better defining what “bureaucracy” really means and how it is perceived by all the parties involved would be a worthwhile pursuit. Nonetheless, the perception that bureaucracy is in some way, shape, or form hindering the process exists, and this can trickle down all the way to the implementation of technical measures.

C4.3: Industrialization of Privacy Compliance

We have seen the industrialization of privacy consultancy, if you like, from technical nerds, or legal nerds doing privacy work, to becoming sort of more productive, revenue driven and into an industrialized space to a certain extent. (I7-L)

The theme introduced by this challenge is truly interesting, and it is one mainly motivated from the insights of one particular interviewee with experience spanning many years. The sentiment is also alluded to by other interviewees. What is really meant by this “industrialization” will be expounded upon soon. Interestingly enough, the “challenge” presented here is really a matter of perspective; what some may see as a challenge, other could perceive as a positive and beneficial development. For the former reason, it is included in this work as a challenge, but it certainly must not be so.

While the introductory quote refers more specifically to the field of work in which I7-L works, this interviewee goes on to make clear what is meant, now incorporating the entire privacy community:

It really became from a one person practice sort of standard to like an industry of organizations who have been building software around privacy compliance, we saw really a standardization of products that have had to share the mass market with GDPR. And we also have seen those organizations emerging, like BigID and OneTrust and Usercentrics are now becoming really larger organizations. So that’s what I call the industrialization of the industry.

Perspectives like this are so valuable in the way that professionals with decades of experience in the field can best follow such a development. On a side note, a more in-depth study into this matter would be a very interesting endeavor.

Diving deeper into the two statements from I7-L, the main narrative lies in the people and roles involved with this concept of privacy, or rather data protection. Before the dawn of sweeping privacy regulations such as the GDPR, the practice of “privacy compliance” was seemingly much more localized, with individual and specialized experts. The big change, perceived to be GDPR, fueled the transition to a “mass market”, with the entrance of specialized organizations now. At the center of the purpose of these organizations is privacy compliance, and at the center of this is the “software”. In short, “It’s now becoming a private sector issue.” (I1-T). As such, an industry was created.
The positive spin on this industrialization can be quite self-evident. Rather than existing in isolated, localized niches, the idea of privacy and data protection have become industrialized in the sense that its necessity and importance has become a global issue. Data processing must be performed in a compliant manner, says the law. And better yet, the increasing attention given to the matter has bolstered the development of technologies, the technical measures to facilitate data protection. Finally, the “standardization” that is mentioned can also be judged to be a step in the right direction.

It is at this point that the potential challenge, or drawback, of this so-called industrialization becomes apparent. Specifically, this occurs in the way that industrialization can also be seen as commercialization. A brief insight into this:

I think it’s a huge gap. If you look at especially the European front, it was kind of pushing for more of a human rights aspects behind it. Whereas it really is [now] more of a commercial and operational risk. (I9-T)

The gap illustrated here places this challenge as a precursor to the final challenge that will be discussed in this work, namely C4.8. In the talks with other interviewees on this subject, this notion was hit at different angles. In essence, if one traces back this industrialization to where these privacy experts (“nerds”) where the main proponents of privacy compliance, here the privacy and the data protection were truly center, and this idea of compliance was a means to their achievement. In the lens of commercialization, the end goal is now achieving compliance, with technical measures for privacy and data protection as the means to do so. The distinction here is profound, and it is also something that will play a significant role in the next challenge.

C4.4: Inequality in Privacy Compliance

You can definitely be 100% in compliance, but not be doing the right thing from a privacy or ethic or even a legal perspective. (I9-T)

So this thing has teeth. But the tiger doesn’t want to bite. (I10-LT)

The challenge posed by C4.4 is a complex one; at the same time, it is clearly very important and on people’s minds, as this received the most occurrences out of any other challenge. The premise of the challenge is rather straightforward, that the “main challenge is to treat everyone equally when it comes to requirements” (I2-T) of privacy compliance. Under the hood, though, this challenge can be tackled from many angles. As almost an alternative title to inequality can be considered the term bare minimum technical measures, which points to one extreme of the challenge. Seeing where such an idea originates can be done by first building up the challenge.

As a reiteration that comes as the summation of some previous challenges, the road towards the demonstration of privacy compliance may not be easy. In particular, choosing the correct technologies and implementing the appropriate technical measures may present a challenge in of itself. Beyond this, however, a novel challenge is presented in the light of an ever-evolving
data protection landscape. In the words of a privacy engineer working at the crux of this challenge:

So by understanding the technical measures, it’s easy to implement a solution that satisfies the regulation. It’s not easy to implement a technical measure that actually gets ahead of it or is forwards compatible enough to maybe incorporate some changes in the regulation. (I4-T)

An added layer of uncertainty comes with the contrasting idea of achieved compliance and true data protection, as exhibited when I9-T says, “We might be in compliance, but that doesn’t mean that we are actually doing the right thing.” And of course, the variability of the process once again becomes a factor: “There is nothing like the perfect data privacy, or data privacy compliance. I think it’s always depending on what the company is doing.” (I12-L).

The real point of investigation as it pertains to C4.4 is how organizations perceive and react in the face of these challenges. As it turns out, there is no harmony in this regard, i.e. the approach towards the implementation of technical measures is quite uneven. One interviewee provides an educated estimation of the state of things:

I’m pretty sure that only 30% of companies really, really get a good handle on it. And then there’s another 50%, somewhere in the middle, and there’s 20% who still haven’t done the thing, and which is also fine, because by now it’s pretty predictable when you get caught and when you don’t. (I5-LT)

The latter part of this statement will be addressed shortly, but the former is very revealing, particularly in the way that another separate interviewee provides almost the same evaluation of the field, formulated in a different way:

There are a lot of companies who do the bare minimum. And basically, the bare minimum usually is something that can be visible from the outside. So they have a good privacy policy, they have some kind of good checkboxes on their website. So the first thing that somebody coming to the organization will see. But then there’s a mess inside, right? There’s no internal procedures, nobody understands or cares what kind of vendors that are onboarding or something like that... the next level would be that, okay, we have something, we have some kind of internal procedures, we have some kind of policies and so on. But those are basically kind of living on paper, they’re not actually used or implemented in daily business activities... the top level and the level that should be there for most companies, especially those who are bigger companies, and operating with a lot of debt, a lot of that is kind of really thinking about how we need to change our processes, how we need to adapt our infrastructure or IT systems to really ensure that we’re not just compliant on paper, but we’re implementing all of this in our business activities. (I8-L)

Quite a bit to digest here. First and foremost, the interviewee breaks an organization’s approach towards technical measures into three categories. From “most advanced” to least, these might be summarized as:
7. Challenges

1. Top level – compliance procedures, infrastructure, and “awareness” actively practiced
2. Middle level – procedures in place
3. Bottom level – “bare minimum”, compliant on the surface

An integral aspect to this top level is an active attention to the need for change in processes, and one might argue culture, as previously discussed. I8-L goes on to stress the importance and merit of striving for this top level approach, saying:

I think that you can be compliant not only on paper, but you should also think how you’re compliant in real life and in really dealing with these issues, and then kind of implementing all of the requirements in the business activities as such. So I think that would be kind of the level to strive for.

Here the ideal level is also contrasted with the ideal of being compliant “on paper”, which can be equated with the concept of the bare minimum. On the other hand, truly tackling the issue of data protection is something that demands more attention than achieving compliance alone may require.

The idea of bare minimum technical measures is a topic that several additional interviewees address. I2-T believes that “there are some actors now in the market that fulfill this requirement in a very easy manner”. One might inquire into what kind of internal factors might influence the decision to remain with minimal measures in order to reach compliance. For starters, a lack of proper communication, education about technologies, and an organizational culture that values data protection could all influence the decision, as introduced in the previous categories. Another aspect of this matter is the difference between legal and technical interpretations of what might be adequate measures, as hit upon here:

There’s a very big difference between a legal analysis or assessment and a technical privacy implementation. And things that might be legal, according to regulation might not actually be things that are privacy preserving. (I9-T)

As supported by this statement, the recommended measures as result of a legal assessment may not be directly in line with that which is believed to be the best privacy-preserving solution. At the end of the day, the implementation of technical measures for privacy compliance presents a significant overhead and as discussed, this can be a major factor in the whole matter, as emphasized by one interviewee:

Privacy protection is always a kind of overhead or protocol and all the companies want to do the minimal things that are needed. We cannot say that we just, we sacrifice everything just to protect the user. But that’s from this aspect. So what really compliance can bring us it’s not that much. (I15-T)

The last sentence is thought-provoking, and it segues into the next stage of the discussion. The investigation into what may be causing an inequality in privacy compliance can also be viewed as taking root in external factors, specifically the enforcement of privacy and data protection regulations. On one hand, the threat of fines can be a good motivator to implement
7. Challenges

sound technical measures. This, however, will only be true if it is met with an equally strong enforcement. Put more eloquently:

If you don’t enforce the law, like the Irish DPA, then there is de facto no privacy law, no data protection law, nothing, because it’s not enforced... Why put enormous resources into something that nobody looks at? (I10-LT)

One does not have to look far to find examples of enforcement, such as the one directly referenced in the above statement, pointing to the the $267 million fine imposed on WhatsApp by the Irish Data Protection Commission in September 2021 [77]. Even the title of this article, though, indicates a potential flaw, namely the “willingness to issue large penalties”, i.e. pursue larger organizations. To this point, I10-LT provides an interesting insight:

This is kind of forcing people to unproportionally invest to achieve compliance. And even then, it’s very hard to do. Given the enforcement pressure, it’s much easier to do nothing and fly under the radar. Because you have no realistic goal.

This echoes a statement from I5-LT given above, claiming that for some organizations, it might be easier to “fly under the radar” rather than invest in proper technical measures. Again, this all boils down to a risk assessment, i.e. the risk of enforcement versus the cost of implementation. Indeed, this tiger has teeth, but in many cases, it may not be worth it to bite – and some organizations may be aware of this.

In the course of this discussion, one may begin to see that in many cases, the approach towards privacy compliance does not exist on a level playing field. In this light, one interviewee even warns of “over-compliance” as a potential side effect, saying that if “you’re overly compliant, less compliant companies can get away with it, and actually benefit from profits, you should be making such an issue.” (I14-L). A incredibly intriguing concept, and one that once again places the implementation of technical measures on a sliding scale. In the case where the degree of data protection far exceeds what is actually required for compliance, one may argue (privacy aside) that superfluous resources were expended.

The challenge presented here calls for further investigation, one that necessitates a comparative study of organizational approaches and attitudes towards privacy compliance. At a high level, the presence of an inequality in the process of privacy compliance can be concerning, calling for a better way to classify and measures levels of compliance, as well as a reflection of this matter in the privacy regulations themselves.

C4.5: What is Privacy?

Challenge C4.5 represents arguably the most abstract of the identified challenges, with its foundations in the age-old question holding the title of this section. Chapter 2 discussed at relative length the myriad of ways in which privacy can be interpreted, from a theoretical, personal, or even philosophical standpoint. In addition, a complex dimension is thrown in the mix when one considers the idea of privacy in light of data protection, thus data privacy. The argument here, then, is that with such a multi-faceted and sometimes controversial nature, the complexity of privacy almost necessitates an extra layer of challenge for privacy compliance.
7. Challenges

It must be stressed, as in Chapter 2, that privacy in its purest form is not a novel concept. 111-L would agree: “Privacy is nothing new, right? It didn’t kind of come from nowhere in 2018 and has been here for since mankind.” This non-withstanding, the notion of privacy has proven to be quite hard to define, consistently and unilaterally. Whether this is or ever will be possible is another question. Surely, one could certainly consult the Wikipedia definition [78], which states “the ability of an individual or group to seclude themselves or information about themselves”. Or perhaps one could reference one of a plethora of philosophical works on the matter. Even the IAPP, an organization whose mission roots itself on the definition and promotion of the privacy profession, must begin its definition of privacy with a caveat: “Well, it depends on who you ask.” [79] Perhaps the point is clear, but the fact remains that “this fuzzy concept of privacy” (I2-T) could have significant implications on the implementation of technical measures for precisely its protection.

When it comes to technical measures, one may argue that in order to know what to implement, one must have a good idea of what privacy means, in the technical sense. One challenge arises at this point, as described when one interviewee claims, “I don’t think everyone has a consistent definition of privacy, or even privacy engineering.” (I9-T). And this does not necessarily only include the technical persons involved with the process of privacy compliance. This again takes root in the complexity of privacy and accordingly, data protection, as illustrated here:

Every time we just start to define privacy, we’ll start by fighting or discussions and so we can’t apply any consistent definition. So that’s it, there’s no definition of privacy, you can view privacy from the legal aspect, from the ethics aspects and technical aspect. (I15-T)

With all these possibilities in the air, the question of what is privacy must be addressed even before the question of technical measures can be tackled.

In terms of thinking about the quantification of privacy in the technical sense, the research field has certainly not come short of providing a plethora of definitions. In a recent survey on technical privacy metrics [80], the authors identified over 80 existing metrics, categorizing these into eight distinct types of metrics. In addition, other characteristics are taken in consideration, as well as the categorization of privacy domains. With this incredible diversity of metrics for privacy in the technical sense, it may be no wonder that beginning to reason about technical measures for privacy compliance can be quite overwhelming. Moreover, relating directly to the core of the challenge here, how and to what degree these technical definitions line up with other definitions (sociological, philosophical, etc.) is unclear, let alone how these metrics compare to each other. Thus, this challenge is becomes in part one of the “agony of choice”.

The complexity does not end there, though. As alluded to in Chapters 2 and 3, the inherent differences in the mindset and practice of the legal and technical fields has quite understandably led to differing definitions of privacy. As a results, attempts have been made to harmonize these concepts, such as through the work of [81]. This work does address the fact that even beyond the legal and technical spheres, cultural and personal factors also come into play. Admittedly, though, this work only represent an introductory, cursory attempt at
the consolidation of the technical and legal concepts of privacy; quite clearly, much work remains to be done.

Building upon the aspect of culture as previously introduced, the challenge in discussion here gains yet another dimension. The premise is that different beliefs, values, or opinions on privacy will affect the way in which technical measures are approached. In one account, these differences can be divided into two distinct categories, underpinned by culture:

There are two drastically different approaches to compliance that are cultural... in the US, we have no technical measures, there’s just not a thing. It’s what methods and processes are we going to put in place, from an organizational corporate standpoint, to reduce risk... from a French or Spanish perspective, but I know that the German perspective is the same, we will do whatever the law says. We don’t actually care what the risk is, if the law says that we should implement technical measures, we will implement technical measures, we won’t ask. (I3-L)

In one singular statement, many of the overarching themes presented in this work are synthesized to prove one major point: technical measures predominantly become a matter of interpretation. This interpretation, in turn, is very dependent on risk tolerance, organizational decisions, and of course, cultural values. Drawing from the many insights seen so far, privacy compliance begins to embed itself in cultural norms and values, extending far, far beyond the original letter of the law.

To better ground this challenge, it can summarized in a concise manner. Privacy compliance provides the pathway(s) to true data protection and privacy. Technical measures, when properly implemented, are the vehicles to achieve such goals. Ultimately, however, the drivers of the whole matter are the many roles involved in the privacy compliance structures – how they drive, which roads they choose, and whether the end destination is the same for all – this is the fuel powering the whole structure and moreover, wherein challenges may lie. At the very core, what privacy means to the one or the other is the true question.

C4.6: Privacy, Data Protection, Security

The challenge here is brought up as the result of its mentioning from several interviewees. Essentially, the idea behind this challenge is that privacy is often conflated with security, when this should not be the case. Admittedly, this is done also in some of the direct quotes included throughout this work. On top of this, the distinction between data privacy and data protection may not always be apparent. It is for this reason that the author would like to emphasize that no viewpoint is necessarily “correct”, but the one described in this challenge presents an interesting side of the story.

The exact interplay between privacy and security is a bit uncertain, particularly in their origin. In talks about the concept of privacy, one interview says that “some people could say it grew from security, even though I’d argue it’s far older” (I4-T). Analyzing this statement, it could actually be the case that both parties are justified in their belief. In a technical sense, i.e. as it applies to the technology industry, the practice of security (data security, information security, cybersecurity) certainly takes the cake as the “older” practice. One may even go
so far as to argue that the security industry is far more mature than the privacy profession. Pertaining to society, though, it could be that privacy actually represents the older inherent concept. Regardless of what the answer may be, the relationship between security and privacy is without a doubt intriguing.

How this is reflected in the privacy compliance process has already been introduced by one interviewee, who calls for a better literacy regarding the distinction between privacy and security. Furthermore, this person sees a fault in some compliance programs:

Don’t put [privacy engineering] under your security office. So that’s another thing that I’ve seen companies do. I wish that more people appreciated the distinction. (I4-T)

This calls to question the underlying nature of how technical measures may be supported. Surely, data security is one thing, but how it applies to data processing is much less clear. On the other hand, data privacy can certainly be viewed in a two-fold manner. Firstly, privacy can be protected by security, i.e. by not leaking private information via breaches. On another level though, privacy in the actual mechanisms of data processing is very distinct from securing data, but rather focusing on the manner in which data is handled. This among others, is a main motivation of things such as Privacy-Enhancing Technologies. To these points, I4-T’s argument gains validity; the literacy is needed to characterize this distinction in a more meaningful way.

On the topic of differentiating privacy and security, the role of the user was also brought into play. One insight here comes with the following statement:

Thinking about how [the individual user] might consider privacy, which can be easily lumped into things like security and safety, they might not necessarily even differentiate these concepts. (I9-T)

The need for better technical literacy (education) seemingly arrives also on the consumer level. A conflation of the two concepts on the implementation level could certainly add to this confusion.

Looking to the literature, clear attempts have been made to differentiate the concepts of privacy and security. One particular work [82] strikes the author as particularly impactful, hailing from the legal side. The author begins right away by acknowledging the frequency by which “legal scholarship tends to conflate privacy and security”. These notions, however, should be kept distinct. In another interesting focal point of this work, the moral ambiguity of privacy (that cannot be claimed for security) leads one to believe that “security flaws are penalized too rarely, and privacy ones too readily”. As this begins to depart from the scope of this thesis, this will not be analyzed too deeply. Its implications, however, can certainly be pondered about with regards to privacy compliance, and its enforcement.

The case with privacy and data protection has merited similar scrutiny. In [83], the two concepts are seen as both formally and substantially distinct concepts, both of which can significantly vary by culture or perspective. In a more technically-centered work [84], though, the distinction between privacy and data protection is not so clearly made, and the two
notions are often mentioned in pair. Yet another work [85] helps to clear this up a bit, essentially marking the role of data protection in data processing to protect data privacy, or simply privacy. Such a relationship was also considered in Chapters 2. As opposed to the case of security, the distinction between data protection and privacy is not as transparent, and their frequent conflation may indeed be justified.

As a conclusion to this argument, it should be stated clearly that the need for security in the dynamic of privacy compliance should not be understated. After all, security ultimately represents the first line of defense against bad actors. Indeed, it is often the case in research works that both are analyzed concurrently. Even so, the technical measures as required by regulation address the compliant processing of data. For data protection, these technical measures must therefore be thought about under the lens of privacy, which facilitates the proper handling of data, in a way that is distinct from data security.

C4.7: Privacy in Modern Privacy Compliance

But there is that gap, and there is that problem of the gap that I at least see, is that we almost have forgotten why we do it [privacy]. (I7-L)

The final challenge introduced in this work is one that can quite possibly be seen as the most “meta-challenge”, for reasons that may soon become clear. In the investigation of technical measures and their role in the whole landscape of privacy compliance (and beyond), it might be easy to lose sight of the basis of the discussion. The immense role that data processing plays in the modern technological industry and the concerns that have been risen because of it - this is predominantly why the issue of data privacy and data protection have even entered the stage. To aid in this pursuit, the requirement of compliant data handling via the establishment of proper technical (and organizational) measures has been seen as the de facto way in which data privacy can be safeguarded. As a result of this, a complex network of regulations, authorities, interactions, processes, and technologies has been construed in light of this methodology. In this dynamic, the challenge becomes when the focus shifts primarily to compliance, rather than to privacy itself; moreover, the true challenge comes when the two do not align.

One area of contention may arise from the belief that compliance to regulation does not necessarily mean that privacy is protected. This contrast is illustrated by one interviewee, saying “I think we don’t violate any privacy regulations. But of course, we cannot say that we are 100% sure that we don’t have any privacy risks.” (I15-T). Interestingly, this almost points to an existing gap between compliance and data protection. Even if one is in full compliance, i.e. not in violation of any regulations, this does not necessitate the lack of privacy risks. From a legal point of view, this sentiment is also expressed, but from a procedural standpoint:

We’re going to put together those checkboxes to do those things. And if they work, or they don’t work, that’s actually not the goal here. The goal here is to show that we were doing what the regulator said. (I3-L)

This directly relates to technical measures, in the way that they might be implemented to “fill
a checkbox” for the goal of compliance. As another way of viewing it, this sort of compliance can be coined as academic compliance, as one interviewee puts it:

A kind of academic compliance, because the law says you should do it. Maybe the lawmakers had different intentions when they wrote it. (I5-LT)

The discussion here almost picks up where “bare minimum” technical measures left off, and they are undoubtedly related. With modern privacy compliance and its requirements and incentives, perhaps the “true” meaning of privacy is becoming lost. On the other hand, though, how can one enforce the protection of data privacy without something like regulations (and compliance)? The challenge is complex.

The question of this meaning of privacy is offered some insight by one interviewee, who claims that the development of the industry over time has led to perceivable changes in this matter. As a synopsis:

What in my view got lost is the real purpose of what we’re doing. So, if you talk to people who have joined the industry in the last three to five years, for them, it’s more really about managing privacy compliance... But this is that piece currently missing. (I7-L)

The sentiment here also comes in complement to the “industrialization” of the privacy profession, covered in C4.3. The ultimate grounds for such an argument, though, rests upon one’s own definition of privacy, which will directly influence whether the challenge here is one at all. I7-L sees privacy in a certain way:

Privacy is about that fundamental right of absence of government, in order for you to participate freely in a democratic society. That is still my current understanding of what privacy is about. I know that the current industry is has taken a completely different route.

This interviewee goes on to acknowledge that such “knowledge has been almost lost, it is considered sort of the old privacy” (I7-L). What, then, may be considered new privacy? In asking many of the interviewees this question, the general answer revolves around proper handling of a user’s data by a data processor. The influence of the GDPR here cannot be missed. For this reason, whether modern regulation or more personal factors enact the greater influence on this challenge is difficult to pinpoint.

Going one step further, the technical measures themselves may be called into question. A technical perspective from the literature states that “Anonymity is not privacy” [86], and furthermore, that much of today’s privacy-enhancing technologies revolve around the former, perhaps not fully addressing the latter. Indeed, this may raise doubt about the idea behind technical measures, particularly the requirement imposed by regulations such as GDPR, which place a particular focus on anonymization. In this debate, one can refer back to the idea of data protection: what is it that really should be protected? Privacy? Alas, [86] poses similar inquiries, claiming that in order to “build meaningful protections for sensitive individual data, we must ask the right questions.” At the center of these questions is the meaning of privacy. In this way, C4.5 and C4.7 are undoubtedly interrelated.
In wrapping up this challenge, one may see the merit of such an argument, but at the same time, it can be hard to justify when the “modern definition” of data privacy, as it pertains to data processing, is “just as correct” of a definition. In this light, the true meaning and motivation behind technical measures for privacy compliance may have not been lost, but merely just shifted. Nevertheless, this challenge is fitting as the last, as it presents a highly complex case which begs for deeper investigation and analysis.

7.5.3. Summary

The challenges identified in Challenge Category 4 are truly best described by their generality, since they cannot easily be assigned to particular interactions, technologies, or even organizations, but rather they apply as general insights into the process of privacy compliance as a whole. The focus in this category was placed on the challenges introduced by the great diversity and variability of the industry, and how the nature of regulations affects this. In response, the mindset afforded towards technical measures can generally differ based upon a spectrum of factors. And above all, this “fuzzy” concept of privacy lies at the background of the entire picture. Particularly with many of these challenges, they are very much a matter of interpretation, and as a result, their status as challenges must be called into careful question. As such, a certain emphasis will be placed on their analysis in the next chapter. Challenge or not, the themes and questions raised here serve as incredibly interesting discussion points, and were held in particularly high importance by many interviewees.

Mapping

Figure 7.4 presents the mapping for Challenge Category 4.

If one had to deduce a particular structure for Figure 7.4, perhaps the best fit would be that of “horizontally clustered”. This for one lies very much in the order with which the author decided to present the challenges, which was to group similar challenges (this was predominantly done for all categories). One can selectively pick out a few examples of this, such as I4-T and I9-T with C4.4-6, or I14-L with C4.1-4. The continuity of some of these mappings across several challenges can speak to the strength in belief of some interviewees behind certain challenge concepts.

A particularly interesting exercise that can be performed with especially this mapping, but also surely with all others, is the construction of challenge narratives. Specifically, this means to build a narrative around the context of several challenges, rather than view them in isolation. One such example is performed for illustrative purposes:

I15-T places emphasis on challenges C4.1, C4.4, C4.5, and C4.7. As a privacy engineer, the importance of privacy compliance must be stressed in the light of sound, innovative technical measures. This, though, requires significant overhead. The decision to meet this overhead upfront is largely an organizational decision, which is affected by cultural, legal, ethical, and technical perspectives on the meaning and importance of data protection. As a result, some organizations may opt to settle for bare minimum technical measures, merely in the pursuit of
7. Challenges

compliance. In this way, compliance can be claimed, but privacy risks may remain. In such, we see that a focus has been drawn away from true privacy, and more towards privacy compliance.

Of course, such a process could use some refinement, and it certainly may not represent the true logic or thought process of an interviewee. Nevertheless, exercises like this, which most certainly include other useful visualizations and such, may be useful to connecting all of the identified challenges into an ecosystem. The context is undoubtedly important.

![C4 Mapping](image)

Figure 7.4.: Challenge Category 4 Mapping
8. Survey Analysis

As outlined in Chapter 4, the survey that was conducted as part of this research comprises of the quantitative analysis stage. Specifically, the strength of each challenge can be judged via the quantification of responses gathered from the conducted survey. For the purposes of this thesis, survey questions which focused on the challenges identified in the previous chapter are the point of analysis. The final section of the survey, pertaining more towards Research Question 3, will be covered in the next chapter. It should also be noted that the particular questions analyzed in this chapter represent a selected subset of the entire survey, i.e. those that merit deeper analysis. For space and brevity reasons, every single survey question will not be analyzed. Appendix B, however, contains the result of all questions not covered in this chapter, in tabular form. The survey questions that are included in this chapter will be split into their respective challenge categories, and further split into sub-categories based upon the response outcome. Before this analysis is presented, first some information to the survey makeup and analysis procedure is provided.

8.1. Survey Makeup

The full set of survey questions can be found in Appendix B, but important information about their relation to the challenges is presented here. In addition, some summary statistics of the survey respondents are also displayed.

8.1.1. Survey-Challenge Mapping

In order to carry out the methodology as described in Chapter 4, the survey questions, or rather statements, were created in the Likert format, with the goal of assessing a survey participant’s level of agreement with a particular challenge. As such, the creation of the survey questions was done following the quantitative analysis, i.e. after the challenges (and their categories) were identified from and grounded in the interviews. To best make this relationship clear, a mapping is presented which identifies which survey questions are pertinent to which challenges. This is important because the quantification of a challenge’s prevalence can only be done with this mapping in hand. Accordingly, Table 8.1 maps each challenge (by code) to the corresponding survey question(s) and their section header in Appendix A. Note that one challenge may have more than one matching survey question. Survey questions appearing in Appendix B but not in Table 8.1 either contribute to an understanding of the survey makeup, to Research Question 3, or simply to general insights.
8. Survey Analysis

Table 8.1.: Survey-Challenge Mapping

<table>
<thead>
<tr>
<th>Code</th>
<th>A2.2.3</th>
<th>I rarely interact with more technically/legally-oriented people regarding privacy compliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1.2</td>
<td>A2.2.4</td>
<td>When interacting with [technical/legal] experts about privacy matters, the process can be slow or frustrating.</td>
</tr>
<tr>
<td>C1.3</td>
<td>A2.2.5</td>
<td>When interacting with [technical/legal] experts about privacy matters, I feel like there is a disconnect that creates challenges.</td>
</tr>
<tr>
<td>C1.4</td>
<td>A2.2.6</td>
<td>I believe there is a need for more and/or better interaction between the technical and legal sides of privacy compliance.</td>
</tr>
<tr>
<td>C1.5</td>
<td>A2.2.7</td>
<td>I believe that in general, there is a lack of [technical/legal] knowledge on the [legal/technical] side.</td>
</tr>
<tr>
<td>C1.6</td>
<td>A2.2.8</td>
<td>Data privacy and privacy compliance are becoming more and more technically-centered.</td>
</tr>
<tr>
<td>C1.7</td>
<td>A2.2.9</td>
<td>There is a need for more technically-minded people in the conversation about privacy compliance.</td>
</tr>
<tr>
<td>C1.8</td>
<td>A2.2.10</td>
<td>Any perceived gap in knowledge or understanding between the technical and legal sides of privacy compliance is a good thing.</td>
</tr>
<tr>
<td>C1.9</td>
<td>A2.2.11</td>
<td>There is a lack of interdisciplinary/cross-functional teams in privacy compliance programs, i.e. a better balance is needed.</td>
</tr>
<tr>
<td>C1.10</td>
<td>A2.2.12</td>
<td>As a [technically/legally]-oriented person, I feel like the makeup of current privacy regulations leaves much of the interpretation work up to me.</td>
</tr>
<tr>
<td>C1.11</td>
<td>A2.2.13</td>
<td>I believe my answer to the question above is the optimal state of things.</td>
</tr>
<tr>
<td>C1.12</td>
<td>A2.2.14</td>
<td>I feel like there is a lack of proper characterization of PETs (how they work, benefits, disadvantages, etc.).</td>
</tr>
<tr>
<td>C1.13</td>
<td>A2.2.15</td>
<td>PETs are actually quite difficult to implement in practice.</td>
</tr>
<tr>
<td>C1.14</td>
<td>A2.2.16</td>
<td>The ability to implement PETs is very dependent on a company’s resources.</td>
</tr>
<tr>
<td>C1.15</td>
<td>A2.2.17</td>
<td>In general, the understanding of PETs requires a sound technical baseline.</td>
</tr>
<tr>
<td>C1.16</td>
<td>A2.2.18</td>
<td>Communicating about these PETs with people with purely legal background is quite difficult.</td>
</tr>
<tr>
<td>C1.17</td>
<td>A2.2.19</td>
<td>There is no clear sense of how PETs relate to privacy regulations.</td>
</tr>
<tr>
<td>C1.18</td>
<td>A2.2.20</td>
<td>I believe there is a general need for better education on PETs.</td>
</tr>
<tr>
<td>C1.19</td>
<td>A2.2.21</td>
<td>I personally am interested in learning more about PETs.</td>
</tr>
<tr>
<td>C1.20</td>
<td>A2.2.22</td>
<td>There is a general lack of technical literacy when it comes to privacy compliance.</td>
</tr>
<tr>
<td>C1.21</td>
<td>A2.2.23</td>
<td>There does not exist a solid technical framework for privacy compliance.</td>
</tr>
<tr>
<td>C1.22</td>
<td>A2.2.24</td>
<td>I believe there is little incentive to put resources into implementing the newest, state-of-the-art Privacy-Enhancing Technologies.</td>
</tr>
<tr>
<td>C1.23</td>
<td>A2.2.25</td>
<td>It is more convenient and/or economical not to put time and resources into implementing sound technical measures.</td>
</tr>
<tr>
<td>C1.24</td>
<td>A2.2.26</td>
<td>I believe that there are many technologies for data protection, yet the awareness and knowledge surrounding them is lacking.</td>
</tr>
<tr>
<td>C1.25</td>
<td>A2.2.27</td>
<td>Privacy compliance doesn’t motivate the innovation of technology in the privacy field.</td>
</tr>
<tr>
<td>C1.26</td>
<td>A2.2.28</td>
<td>When it comes to interpreting privacy regulations, this interpretation comes from the management level within my organization.</td>
</tr>
<tr>
<td>C1.27</td>
<td>A2.2.29</td>
<td>I believe there are many ways to approach privacy compliance, specifically regarding technical measures.</td>
</tr>
<tr>
<td>C1.28</td>
<td>A2.2.30</td>
<td>There is an inequality in the current industry as to what suffices as ‘being compliant’.</td>
</tr>
<tr>
<td>C1.29</td>
<td>A2.2.31</td>
<td>The politics within an organization may affect the degree to which sound technical measures are pursued.</td>
</tr>
<tr>
<td>C1.30</td>
<td>A2.2.32</td>
<td>My organization has an established and easy to understand structure with respect to privacy compliance.</td>
</tr>
<tr>
<td>C1.31</td>
<td>A2.2.33</td>
<td>I believe this structure matches that of peer organizations within my field.</td>
</tr>
<tr>
<td>C1.32</td>
<td>A2.2.34</td>
<td>More focus should be placed on “privacy engineering” within organizations.</td>
</tr>
<tr>
<td>C1.33</td>
<td>A2.2.35</td>
<td>On the whole, I would say legal support is readily available to me regarding any privacy-related matters.</td>
</tr>
<tr>
<td>C1.34</td>
<td>A2.2.36</td>
<td>The implementation of technical measures for privacy compliance can be challenging depending on what systems are involved.</td>
</tr>
<tr>
<td>C1.35</td>
<td>A2.2.37</td>
<td>Privacy compliance can be a bit of a “gray area”.</td>
</tr>
<tr>
<td>C1.36</td>
<td>A2.2.38</td>
<td>When it comes to technical measures for privacy compliance, this largely becomes a financial matter (creates a significant overhead).</td>
</tr>
<tr>
<td>C1.37</td>
<td>A2.2.39</td>
<td>Demonstrating sound privacy compliance can actually boost a company’s value.</td>
</tr>
<tr>
<td>C1.38</td>
<td>A2.2.40</td>
<td>At the core of implementing technical measures for privacy compliance is a risk assessment, which is dependent on organizational culture.</td>
</tr>
<tr>
<td>C1.39</td>
<td>A2.2.41</td>
<td>I believe that the amount of privacy regulations nowadays makes implementing technical measures for privacy compliance convoluted.</td>
</tr>
<tr>
<td>C1.40</td>
<td>A2.2.42</td>
<td>There is a clear need for better “harmonization” of these regulations (and requirements).</td>
</tr>
<tr>
<td>C1.41</td>
<td>A2.2.43</td>
<td>Privacy compliance involves too much bureaucracy.</td>
</tr>
<tr>
<td>C1.42</td>
<td>A2.2.44</td>
<td>All in all, I think recent years have seen the industrialization of privacy (compliance).</td>
</tr>
<tr>
<td>C1.43</td>
<td>A2.2.45</td>
<td>This industrialization is in my view a positive advancement.</td>
</tr>
<tr>
<td>C1.44</td>
<td>A2.2.46</td>
<td>It is often the case with privacy compliance that although compliance can be argued for, true protection of privacy may not be achieved.</td>
</tr>
<tr>
<td>C1.45</td>
<td>A2.2.47</td>
<td>There is such a thing as “over-compliance”.</td>
</tr>
<tr>
<td>C1.46</td>
<td>A2.2.48</td>
<td>In general, I think the concept of privacy itself is quite vague or not well-defined.</td>
</tr>
<tr>
<td>C1.47</td>
<td>A2.2.49</td>
<td>The meaning of privacy is distinct from, and often conflated with, the concept of data protection.</td>
</tr>
<tr>
<td>C1.48</td>
<td>A2.2.50</td>
<td>Being 100% compliant does not imply 100% data protection.</td>
</tr>
<tr>
<td>C1.49</td>
<td>A2.2.51</td>
<td>The true meaning of privacy has been lost in modern privacy compliance.</td>
</tr>
</tbody>
</table>
8. Survey Analysis

8.1.2. Respondent Makeup

The survey received responses from 23 participants (at the time of writing). While this was not necessarily an optimal number, it is viewed as sufficient, at least exceeding that of the interviews. In order to summarize the makeup of the respondents, four demographics will be visualized: role, experience, organization size, and technical versus legal profession.

Roles

To visualize the respondent makeup in terms of roles in the most succinct manner, the privacy compliance structure from Figure 6.1 will once again be put into action. This time, though, only the regions from which at least one survey respondent hails will be highlighted. This will serve to indicate how “complete” or representative of a picture is gained from the survey responses. Figure 8.1 illustrates this – note that as usual, role titles have been generalized, accounting for minute differences in naming conventions.

Figure 8.1.: Respondent Makeup, Roles
Figure 8.1 shows that the survey respondents belong very much to the more “central” roles of the privacy compliance structure, with some of the left out roles existing more towards the fringes. This is judged as a good start, with the obvious ideal to include as many of the roles as possible.

**Years of Experience**

As was done in Chapter 5, it is interesting to see the distribution of the survey respondents with respect to their years of experience in the privacy profession. This is done in Figure 8.2, using the same bins as was done in Figure 5.3.

If one compares the survey respondents’ years of experience to that of the interviewees in Figure 5.3, a very similar distribution exists. The minor difference lies perhaps in the survey respondents displaying slightly more experience (i.e. on the 10+ end), and slightly less from the 0-3 range. Nevertheless, it is interesting to note the similarity – perhaps this is telling of the current privacy professional community in general.

**Organization Size**

A demographic that was inquired about in the surveys was organization size, particularly in light of its perceived importance in some of the identified challenges. Looking purely at the number of employees, the European Commission defines the following categories [87]:

- Micro-sized: < 10 employees
8. Survey Analysis

- Small-sized: < 50 employees
- Medium-sized: < 250 employees
- Large-sized: ≥ 250 employees

Obviously, the lower bound for each category is implied. These definitions were used in the survey, yielding the distribution as shown in Figure 8.3.

Figure 8.3.: Respondent Makeup, Organization Size

Figure 8.3 shows a clear bias towards large-sized organizations, with small-sized not even making an appearance. This is understandable, however, for clearly employees from larger organizations will represent the larger subset of potential survey candidates. Even so, this skew in the numbers should be taken into consideration when analyzing the survey responses.

Technical or Legal

The final background information that will be presented is also something that played a key role in the administration of the survey. In asking whether a survey participant works more on the technical or legal side of privacy compliance, questions regarding the interaction between the two could be better tailored (representing a branch in the survey). The breakdown is visualized in Figure 8.4.

Figure 8.4 indicates a slight majority held by legal respondents, which mirrors the slight majority held by the legal side in the interviews. If one adds up participants from the interviews and the survey, one arrives at the grand total of 17 technical participants and 22 legal participants, with some overlap between the two (these are double-counted).
8.1.3. Analysis Procedure

The quantitative analysis to follow will follow a structured procedure. Firstly, the challenges will be addressed in order, as they were presented (by category) in Chapter 7. As mentioned above, not all challenges may make an appearance here. The included challenges will firstly be divided into one of three categories:

1. **Agreement**: More than 50% of respondents answered with “Strongly Agree” or “Agree”

2. **Disagreement**: More than 50% of respondents answered with “Disagree” or “Strongly Disagree”

3. **Undecided**: Neither of the above two cases apply

This is done to generalize the sentiment towards a particular response, i.e. if it is met with general agreement, disagreement, or neither. In any case, useful insights can be extracted from the overall response.

For the included challenges, the analysis will begin with a visualization of the survey response distribution. A challenge with only one corresponding survey question will be presented simply so. If a challenge has two questions, though, a particular question will be selected and indicated. This is not only for the sake of brevity, but also due to the design of the questions, which can be grouped together for a singular challenge. This should become more clear as examples are given.
As a final part, a brief discussion will ensue to analyze and interpret the presented results. This will be important to giving an initial judgment on the prevalence of each challenge, which ultimately represents the main goal of this quantitative analysis.

8.2. Quantitative Analysis

8.2.1. Category 1: The Technical-Legal Interaction

Note that for this category only, results will be presented separately (two charts) for the technical and legal respondents, in order to best mirror the branching of the survey. The presentation of the survey questions will also reflect this.

Agreement

C1.3 - A2.2.6 Figure 8.5 illustrates the first major area of agreement as expressed by the survey respondents. In total, 18 of the 23 respondents either agreed or strongly agreed that there is a need for better and/or more interactions between the technical and legal sides of privacy compliance. Referring back to the challenge in question, this sentiment certainly validates a certain deadlock existing between the two sides, which presumably can be addressed by better or more interaction. Other than C1.3, several of the other challenges in this first category are tangent to this survey response. Therefore, it is quite impactful in the agreement shown.

C1.5 - A2.2.9 Another point of agreement, as displayed in Figure 8.6, comes with the need for more technically-minded people in privacy compliance. Specifically, this addresses Challenge C1.5, which points to a lack of this technical input. As such, the survey results here
emphasize that in a field where technical measures are becoming increasingly crucial, input from technical experts is likewise very important.

**C1.7 - A2.2.11** A final area of clear agreement that maps to the first challenge category is the validation that the presence of interdisciplinary teams is lacking on the process of privacy compliance. The agreement here confirms the challenge posed by C1.7, as well as unites many respondents in their opinion that more balanced, well-rounded teams are desirable for privacy compliance programs. In this light, this response can be further explored in Chapter 9, where a solution concept directly addressing this is presented.
Disagreement

8.1 Survey Analysis

C1.1 - A2.2.3 The one area of disagreement that one can extract from the survey results comes with the response to the challenge posed by C1.1, namely a rare interaction with the “other side” of privacy compliance. As illustrated by Figure 8.8, the majority of respondents either disagree or strongly disagree with the statement. From this, one may claim that the more prevalent challenge is not rare interaction, but rather the quality or effectiveness of the technical-legal interaction. This is echoed by some of the responses falling into the agreement category covered above. As such, a clear area for improvement is confirmed. It should be noted, though, that the results for this particular question were in no way unanimous – particularly on the legal side, one can see that a considerable number of respondents replied in the affirmative, once again highlighting possible gaps in the field.

Undecided

For this category, it is important to note that while several of the remaining survey questions might qualify as being included, only those that are of particular interest are covered in detail. Specifically, responses that show a clear division of opinion will be highlighted, so as to begin the discussion on why these rifts may exist. This goes for the remaining three challenge categories as well.

C1.4 - A2.2.4 The result shown in Figure 8.9 presents an interesting division of responses, particularly in light of those provided to A2.2.6 (Figure 8.5). Here, one sees that only a small minority of respondents would characterize the interactions with the opposite side as slow or frustrating. Even in the legal case, a significant number of “Disagree” responses were observed. Particularly on the technical side, no clear-cut opinion can be deduced. Ultimately,
this begs the question of what exactly about the current state of the technical-legal interaction leads many respondents to wish for more and/or better interaction.

C1.8 - A2.2.12 The survey responses to question A2.2.12, as exhibited in Figure 8.10, do not necessarily fit into the Undecided category per definition, but rather they are interesting in their underlying insights. Looking at the statement posed, both technical and legal respondents both majorly answered in the affirmative, with also a significant amount of neutral or disagreeing viewpoints. This result is particularly intriguing in the way that it illustrates how both sides believe that the interpretation of regulations falls within their responsibilities. Not only does this bolster the challenge presented by C1.8, but it also speaks
to the highly dynamic, and arguably ambiguous, nature of privacy regulations and the compliance thereto. As such, this survey result indeed fits best into the undecided bucket.

### 8.2.2. Category 2: Technologies

As a preface to this stage of the quantitative analysis, it should be stated that 82.6% of the respondents answered affirmatively to A2.3.2, asking whether they were familiar with Privacy-Enhancing Technologies. Accordingly, one can feel confident that the following survey results originate from experts with a sufficient knowledge base in the topic.

#### Agreement

**C2.1 - A2.3.4** The first area of agreement within this category relates back to C2.1, which speaks of a lack of proper characterization for PETs. As shown by Figure 8.11, many of the survey respondents would agree to this challenge, which helps to validate the complex and sometimes “academic” nature of these PETs.

**C2.3 - A2.3.7** The first survey result shown in Figure 8.12 largely validates a notion that was discussed throughout Chapter 7, namely the complexity of PETs. Specifically, many respondents believe that understanding these technologies requires a sound technical baseline, which lies at the root of the challenge in their usage and communication.
8. Survey Analysis

C2.5 - A2.3.10 Directly related to the previous challenge-question pairing, the result in Figure 8.13 illustrates the strong overall agreement expressed by the survey respondents with respect to the need for better education on PETs. As one can imagine, this goes hand in hand with the requirement for a technical baseline, and one may argue that the two are tightly intertwined. In this way, the proper understanding of the technical measures in question serves a key point in addressing some of the indicated challenges.

C2.9 - A2.3.17 Possibly the most resounding point of agreement within the Technologies category is with the response to the question posed in Figure 8.14. The large majority of agreement responses here serve to confirm a recurring theme that comprised of the core of the narrative in this thesis, that is the crucial role played by education and awareness when it comes to technical measures. As indicated by this particular survey result, many respondents would likely agree that sometimes, the lack (and therefore challenge) stems not from the technologies themselves, but rather the factors surrounding them. Although not covered in this chapter, a similar sentiment is expressed when it comes to PETs regarding resources and finances (see Appendix B, Table B.2).

Disagreement

For the survey questions concerning the challenges in the Technologies category, one set of responses falls into the disagreement category.
One of the only clear sources of disagreement coming from the survey respondents in the Technologies section came with question A2.3.18, which maps back to Challenge C2.10. Figure 8.15 clearly displays how 16 of the 23 respondents answered negatively to the statement provided. This is understandable, as even in the introduction of this challenge, it was predicted to be a potentially divisive point of view. One must not neglect the fact that a handful of respondents agreed to the statement, showing that there is no unified stance on the matter. In the end, it is crucial to acknowledge that such a sentiment indeed exists, and that regardless of what the current state of affairs may be, one must ask what can be done to align the goals of privacy and the innovation of technology.

**Undecided**

Several questions appearing towards the end of the Technologies section fall under the Undecided category, and they are highlighted in the following.

### C2.7 - A2.3.14

An area where seemingly no consensus could be reached was in regards to the presence of a technical framework for privacy compliance, as discussed in Challenge C2.7. Figure 8.16 demonstrates this with no clear majority being observed. Upon further reflection, one may begin to make sense of this result, since there is certainly not a complete lack of a technical framework, but perhaps only the lack of a widely usable and accepted one. It is this discrepancy that could be
the cause for division shown in this survey response. As already stated, more work definitely needs to be done in order to study this challenge with greater rigor.

C2.8 - A2.3.15-16 A very interesting pair of results comes from both survey questions which correspond to Challenge C2.8, referring back to the challenge of incentive to invest into PETs. Beginning with the result presented in Figure 8.17, one observes a pretty even split between all response options, showing a clear undecided result. Interestingly, this almost mirrors the challenge itself, in the way that being incentivized to invest in sound technical measures is ultimately a personal, subjective matter. While for some the motivation may be largely intrinsic, for others a clear external motivation may be missing.

Looking now at Figure 8.18, the result is quite surprising in the way that more respondents provided a response of agreement than that of disagreement. Even with this, the amount of neutral responses very much adds to the undecided nature of the question. The statement posed in the survey is admittedly quite divisive in of itself, but the responses to it emphasize a clear and present challenge that privacy compliance faces. Regardless of motive, if it is indeed more convenient and economical not to invest time and resources into technical measures, the very basis of the compliance process is in danger. Therefore, the verification of the challenge posed here has significant implications, ones that also tie in directly to the challenges of the next category.
8.2.3. Category 3: Organizational Factors

Survey questions falling under the category of Organizational Factors received many responses in agreement, showcasing the pertinence of several of the challenges in this category. In addition, some disagreement and indecisiveness to the challenges also appear.

Agreement

C3.2, C4.1 - A2.4.5 Survey question A2.4.5 was created in relation to Challenge C3.2, but it is also very clearly relates to C4.1, or the challenge of privacy compliance in a variety of “settings”. The response displayed in Figure 8.19 shows a near unanimous agreement to the proposed statement, highlighting the fact that privacy compliance is indeed complex, and that there is no template solution to it. As a result, the influence of the organizational factors discussed in Chapter 7 becomes very important, as made salient by the next two survey responses. This response in particular is also bolstered by the overwhelming agreement to A2.4.13 (see Table B.2).

C3.2, C4.4 - A2.4.6 Another important insight comes from the very strong agreement (Figure 8.20) to A2.4.6, pointing to the existence of an inequality in what it means to be compliant to privacy regulations. Not only does this clearly tie back to Challenge C3.2 again, but it also forms the basis of the “bare minimum technical measures” in C4.4. Particularly with
8. Survey Analysis

this and the previous survey result, an analysis is made complete via the inclusion of the third and final survey question mapping to this question set, discussed next.

C3.2 - A2.4.7 The responses exhibited in Figure 8.21 also indicate a near unanimous affirmative response, and this is very telling for a few reasons. Firstly, the response here lines up very well to the previous two questions, which were created to all map to Challenge C3.2. Therefore, the consistency in response is certainly present. Secondly, and arguably more importantly, the statement posed in this question refers back to one of the more emphasized points of Chapter 7, which is the crucial role played by organizational culture when it comes to privacy compliance and technical measures. This importance is without a doubt echoed by the survey response here, validating the prevalence of the challenge posed by C3.2, and all its related challenges.

C3.4 - A2.4.10 An interesting result comes with the majority of respondents agreeing to the statement that more focus should be placed on privacy engineering within organizations (Figure 8.22). Although the challenge brought up in C3.4 of the lack of privacy engineering was only mentioned by a few interviewees, the survey responses show that this challenge is indeed quite relevant. As a result, the merits of a focus on privacy engineering for the privacy compliance
process are preliminarily confirmed here. The next step is the inclusion of privacy engineering as a distinct solution concept, covered in the next chapter.

**C3.7 - A2.4.15** The result shown in Figure 8.23 is worth mentioning in the way that it shows a strong agreement, but in a way that highlights a particular aspect of Challenge C3.7. In the introduction of this challenge in Chapter 7, it was noted that the financial nature of privacy compliance does not necessarily need to be negative, but rather the demonstration of compliance can actually increase an organization’s value. As illustrated, many of the survey respondents would certainly agree to this. The flip side to this argument surfaces in the ensuing Undecided section.

**Disagreement**

Within the Organizational Factors subset, only one survey response set falls under the Disagreement category.

**C3.1 - A2.4.4** Coming in with a slight margin of disagreement is the response shown in Figure 8.24, which maps back to Challenge C3.1, or the role of management in compliance decisions. Although many respondents disagree with the statement that management does much of the interpretive work, there still remains many neutral or even some affirmative responses. In total, this very
much reflects some of the meta-insights learned in the interviews, chief among them that there is no bona fide privacy compliance structure distributed across the field. As a result, the role of management may vary, especially when factoring in the organization’s size as well as the data processing activity in question. Nevertheless, an insightful survey response.

**Undecided**

**A2.4.2** A survey result that does not strictly map back to a particular challenge (possible closest to C3.3) comes from one of the “introductory” questions to the Organizational Factors section. As shown in Figure 8.25, it is interesting to observe the relative undecided distribution of responses with regards to interaction with the DPO. Above all, this shows both the complexity of interactions that take place, as well as the plethora of structures, in privacy compliance programs.

**C3.7 - A2.4.14** The survey result illustrated in Figure 8.26 also pertains the Challenge C3.7, but this time the sentiment towards privacy compliance a financial matter is clearly more undecided. While the number of affirmative responses appear on the surface to hold the greatest majority, the number of neutral or negative responses serve to balance out the results. As a cursory analysis, one can definitely attribute this distribution to the variability that can be observed in regards to privacy compliance approaches. Whether or not demonstrating compliance becomes a financial
burden can be a result of a number of organizational factors; regardless, this result most certainly merits to be included here.

8.2.4. Category 4: General

The analysis of the final challenge category presents an interesting case. More so than the previous three categories, the survey results from this category prove to be quite undecided, barring a few questions. With this in mind, the clear cases of agreement or disagreement are covered, followed by a few select undecided results.

Agreement

C4.1 - A2.5.2 The first source of agreement comes with the statement calling for a need to harmonize the increasing number of privacy regulations existing today. This comes in response to Challenge 4.1, which poses that this number can create challenges for privacy compliance. Of course, the agreement exhibited here (Figure 8.27) is only the beginning, and the question as to what exactly can be meant (and accomplished) by a “harmonization” of regulations is certainly up in the air.

C4.6 - A2.5.10 The result shown in Figure 8.28 is one that is also closely mirrored by the set of responses to A2.5.6 (see Appendix B). In addition, it hits at a notion addressed by Challenge 4.6 and other, namely of the distinction between privacy, compliance, and security. At the core, it is largely agreed upon that...
achieving compliance does not necessitate the true protection of data privacy; moreover, this would be extremely hard to equate. In the end, this exposes a highly complex dynamic, as well as a potential area for further scrutiny.

Disagreement*

C4.3 - A2.5.5 Question A2.5.5 comes as a follow-up to A2.5.4, in which 73.9% of respondents agree or strongly agree that recent years have seen an industrialization of the privacy compliance field, mapping back to C4.3 which see this change as a challenge. Figure 8.29 in turn displays that a similar majority agrees that this development is actually a positive change, thus almost debunking C4.3 as a challenge, but rather as a merit of recent changes in privacy compliance. This is a fascinating initial result, one that certainly begs further investigation.

Undecided

This final analysis section will feature two survey questions mapping to the last challenge category, in which very even splits were observed among the available response options.

C4.2 - A2.5.3 The responses shown in Figure 8.30 answer to one of the arguably more divisive challenges, namely C4.2, or the challenge of bureaucracy in privacy compliance. The responses are quite evenly distributed between strongly degree down to disagree, showing a relatively wide spectrum of opinions on the
matter. As one must take a largely subjective stance on this particular statement, the difference in responses is understandable. As a concluding point to this particular subject, the mere presence of such a sentiment and the fact that a significant amount of respondents agree to it at the very least confirms its relevance to the core of this thesis – and hopefully to that of future works.

C4.7 - A2.5.11 The final survey result included in this analysis is displayed in Figure 8.31, which maps to Challenge C4.7. The even distribution here does not need much explanation, as the underlying challenge being investigated is also a very subjective one. In the end, one can comfortably postulate that the privacy professional community would be quite divided on this matter, especially due to its very diverse makeup in terms of years of experience. The story behind this survey result must not be neglected though, and it provides an excellent starting point for future changes and improvements.

8.3. Complete Survey Results

The complete survey results, including those not mentioned in the quantitative analysis here, are presented in Appendix B, specifically in Table B.2. As a final point of analysis, the survey in total received 706 affirmative responses, 257 neutral, and 247 negative. These numbers can be extracted from the bottom of Table B.2. Broadly speaking, one can say that the challenges presented in the survey were agreed upon more often than not, indicating the prevalence of the identified challenges in Chapter 7. Finer analysis of these numbers can and should be done, given the complete results, in order to form a more complete and verifiable picture.
9. Solution Concepts

In the course of the interviews that were carried out, a secondary goal in addition to identifying the practical challenges in the implementation of technical measures for privacy compliance was to go one step further, guided by Research Question 3. In particular, a point was made not only to elaborate upon the challenges, but also to brainstorm some possible solutions to them. In the scope of this thesis, these ideas are referred to as solution concepts, denoting both their preliminary nature as well as their potential to address the challenges at hand, not necessarily solve them. At this point it is crucial to acknowledge that many of the challenges introduced in this work are quite complex, and they are certainly not ones that can be “fixed” quickly, let alone during the timeframe of this thesis. The goal here, then, is to begin the discussion around these concepts, particularly in their connection to specific challenges. Secondly, the degree to which privacy professionals agree with such measures will be gauged in the latter part of this chapter, aided by the survey results.

9.1. Solution Concept Overview

A cursory overview of the solution concepts is given in Table 9.1. Note that for the coded concepts marked with an asterisk (*), these concepts were not included in the survey as options, either because of their singular appearance in interviews (S1,2,4), or inclusion as a solution concept after the survey distribution had already started (S3,5).

9.2. The Concepts, Introduced

The solution concepts listed in Table 9.1 are now briefly introduced and discussed. Depending on how much support these concepts may have initially received, their introduction may merit lengthier discussions than others.

S1: Bridge the Gap

By this point in the reading, one may have noticed the preference given towards the usage of the term gap in the description of many challenges. This was particularly true in Challenge Category 1, in which a majority of the challenges can arguably be traced back to a perceived technical-legal gap. It is here where the first solution concept finds its ground.

A first way in which S1 can be useful to the topic at hand would come in the form of research dedicated to the understanding of technical measures for privacy compliance by both sides. A number of works following this general template of comparative studies between
9. Solution Concepts

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1*</td>
<td>Bridge the Gap</td>
</tr>
<tr>
<td>S2*</td>
<td>Context Matters</td>
</tr>
<tr>
<td>S3*</td>
<td>Certification</td>
</tr>
<tr>
<td>S4*</td>
<td>Privacy by Design</td>
</tr>
<tr>
<td>S5*</td>
<td>Cross-Functional Teams</td>
</tr>
<tr>
<td>S6</td>
<td>Mapping of PETs</td>
</tr>
<tr>
<td>S7</td>
<td>Educational materials about PETs and privacy</td>
</tr>
<tr>
<td>S8</td>
<td>Raising Awareness</td>
</tr>
<tr>
<td>S9</td>
<td>Better libraries for privacy tools</td>
</tr>
<tr>
<td>S10</td>
<td>Technical framework</td>
</tr>
<tr>
<td>S11</td>
<td>Privacy compliance KPIs</td>
</tr>
<tr>
<td>S12</td>
<td>More guidance from supervisory authorities</td>
</tr>
<tr>
<td>S13</td>
<td>More audits</td>
</tr>
<tr>
<td>S14</td>
<td>More collaboration</td>
</tr>
</tbody>
</table>

Table 9.1.: Solution Concept Overview

Technical and legal concepts have already been cited in this work, such as with [15], [49], or [81]. Similar investigations into some of the crucial concepts involved in the process of privacy compliance, for example privacy and consent, could be excellent first steps in formulating a hybrid technical-legal understanding of “technical measures”.

Another bridge to be built comes with finding the balance between regulatory requirements and technology, a different sort of technical-legal gap. This is promoted by one particular interviewee:

In fact, we need to come down with the regulation to be more realistic. And we have to kind of bring technology up to speed too. Privacy aware or data protection aware. (I10-LT)

The main questions here would be how to make regulation more in line with today’s technology (rather than simply “state of the art”), while still being encompassing enough to serve as effective regulation. At the same time, it must be achievable to implement such technology.

Indeed, there may exist many a gap to be bridged, and this is to be expected from a relatively “young”, and certainly dynamic, field. The start towards this solution will most likely come with the continuance of research that really dives into the industry, gaining perspectives from all sides.
9. Solution Concepts

S2: Context Matters

In the whole discussion on technical measures for privacy compliance, one large aspect that has largely been ignored by this thesis, and arguably by the regulations in general, is the notion of context. Specifically with this work, the context or domain in which these challenges may occur and differ was not considered. Reigning in a concept first introduced in Chapter 3, someone like Nissenbaum [33] would certainly argue for the importance of context in discussions such as these. And reasonably so – technical measures will be crucial in some data processing contexts, arguably less so in others. The representation of these differences has largely been pushed down to organizational decisions and risk assessments. A more universal guideline may be needed.

One concrete way forward to incorporate better this idea of context into the process of privacy compliance is shared by one interviewee, who champions the use of knowledge graphs:

Why do we use knowledge graphs? Because those are the only tools in informatics that provide context. And that’s the only way you can express the context that you need in the legal environment, for interdisciplinary research. (I10-LT)

How exactly the use of such graphs would ultimately lead to guidance on decisions for technical measures is unclear at the moment. Their potential to integrate contextual knowledge into the process presents an enticing avenue for future research, one that would certainly diverge slightly from the current lay of the land in privacy compliance.

S3: Certification

The topic of certification, especially those offered by the IAPP [88], often came up in the interviews as an important step forward on many fronts. Thus, the promotion of certification could be useful to addressing several of the challenges identified in Chapter 7.

Certification can without a doubt be considered in conjunction with the solution concept proposed by S1. Specifically, if more of the technical roles involved in privacy compliance strive to become certified, they can likely make more sound, confident decisions regarding the implementation of technical measures. I2-T agrees, saying that certification “helps you to better read the law and interpret the law and also to better create things like statements for consent”. One important aspect here is the potential increase in legal literacy offered by certification programs, which in turn allow technically-educated people to also think about these technical measures in a legal light. Such cross-thinking is very much needed.

Another benefit of certification comes face to face with the challenge of lacking technical input in privacy compliance. A major first step in addressing this challenge is equipping the technical side with the appropriate knowledge to be able to enter the discussion. In other words, “I think [greater technical input] will become standard with certification schemes”, says I7-L. At the very least, certification allows people to push the boundaries of their technical (or legal) bubble and gain differing perspectives.

On that note, certification also works in the opposite direction. A legal interviewee says that “the primary education for these [technical] tools are from the certification and the
courses which we do” (I16-L). In this way, certification programs serve as an accessible route for continuing education, certainly not replacing education through degree programs, but providing crucial cross-exchange in a more compact manner.

In order to enact such a solution concept, encouragement to participate in these programs and to become certified should become commonplace for the many parties involved in privacy compliance. With these, one can hope to expect more effective communication, and generally, an increase in cross-domain knowledge, which certainly cannot hurt.

S4: Privacy by Design

But that’s really the way to go about it going forward. Privacy first. (I1-T)

The quote above is quite straightforward in its call for Privacy by Design, by default. In many ways, the challenge and complexity of privacy compliance could be greatly mitigated if considerations about data privacy and data protection are inherent to the design of systems and services. Technical measures, on the other hand, can often take the form of measures implemented “after the fact”, i.e. in order to reduce privacy risks. In Privacy by Design, this is built in, so to speak. This concept is even promoted in the GDPR, with the usage of “data protection by design”. Such design practice is naturally easier said than done, and its true mastery can only be achieved with the proper technical knowledge, as well as the organizational culture to back its implementation. Its ideals, though, should certainly become standard practice going forward, regardless of what is required by regulations.

S5: Cross-Functional Teams

You need to bring the right people together, virtually at the same table... Otherwise, you live in two parallel worlds. (I5-LT)

In many points throughout Chapter 7, particularly in C1.7, it was described how a lack of interdisciplinary exchange in the form of cross-functional teams could lead to challenges in privacy compliance. The central (missing) aspect here is that in an endeavor such as the implementation of technical measures, where the inter-dependency of multiple fields is intrinsic, the right people do indeed need to come together. This notion was quite strongly reinforced in the interviews, showcasing the potential effectiveness of cross-functional teams as the norm, not the exception.

The benefits of a cross-functional team in the context of privacy compliance is hopefully clear at this point. To make this more concrete, a series of similar statements from completely distinct interviews may best exhibit their merit:

It’s critically important, because if you don’t have people from different backgrounds, trying to pick up the new background, you’ll never build meaningful intersection. (I4-T)

I think you have to kind of meet in the middle, because it’s also my duty to explain my my legal concerns to this person in a plain manner. In the same way, as that
9. Solution Concepts

person might explain, IT issues to me in a plain manner, so I think it’s kind of just meeting in the middle and understanding that, okay, we are thinking or dealing with the same issue, but from different sides. (I8-L)

I definitely think there needs to be more of a cross functional team. Because if you’ve only got legal people on it, they might not necessarily understand some of the more technical concepts. And you need a mix of I guess, legal technical, a few other people because everyone sees it differently. And I think you can challenge each other more, which I think makes for more successful team then like everyone with the same sets of skills. (I14-L)

Some interviewees also add to the discussion by describing a sort of symbiotic relationship both necessitated by the requirement for technical measures and fostered by the promotion of cross-functional teams. The payoff for technical persons to have legally-oriented teammates is clear:

    I mean, you don’t have to have a team of lawyers or something. But already having one person with a legal background in your security or privacy team, I would say that can pay off depending on the industry where you’re operating. (I2-T)

On that same token, the legal roles involved also need specific information from technical sides, expressed through the elaborate analogy of system specifications as a “book”:

    So when I’m thinking about talking to technical people, I need to understand, well, how does the door open? And where are the pieces of paper located? And how could someone physically or you know, technologically, but how could they get in? How could they take the information? If they took it? Is the book glued shut? Or is it encrypted? Or could I open it up and see the data on the page? (I3-L)

This sort of cross-disciplinary exchange needs to happen “at the same table”, for optimal effectiveness and more importantly, for breaking down any perceived barriers in mindset or perspective. At the end of the day, it “takes good communication between the between the teams and kind of working on the same issue from two sides to really solve the issue” (I8-L), and the reduction of physical (and metaphorical) distance is a fine start. Thus, it is a truly “a two-way relationship” (I14-L).

I15-T expands the scope of cross-functional teams as not only requiring “somebody to understand the law and also understand the technical”, but also reigning in “the support from the Data Protection [Authorities]”. And this fits into another description of “a cross functional team that understands laws in order to get companies to comply with these laws” (I3-L). Ultimately, the purpose of such a team can surely be viewed as a “bridge” between people of different backgrounds, but also as a multi-faceted tool for effective compliance procedures.
In conclusion to this solution concept, the expressed desire for more cross-functional teams is there. Of course, the presence and potential for such teams can be largely organization-dependent. An implicit advantage of these teams, though, is that they need not be large multi-disciplinary efforts, and some of the insights provided above point towards simple, yet effective individual cross-communications. At the basis, this solution concept champions the worthiness of structured, open, patient, and collaborative relationships between the many parties involved in the process of privacy compliance.

S6: Mapping of PETs

The challenge of determining the relationship of PETs to modern regulation was discussed in C2.4, and will only be reiterated briefly here in the formulation of this solution concept. Essentially, the inherent complexity and “academic nature” of PETs can make their role in the landscape of technical measures for privacy compliance slightly unclear. As such, a comprehensive mapping of Privacy-Enhancing Technologies is needed in order “to find some match between the technology and compliance issues” (I15-T). While work on the characterization of PETs is arguably farther ahead, the role in the context of compliance should become a focal point moving forward. One interviewee sheds some light on how this might proceed, namely to the need to

...extract the core of the requirements from the regulation. And then... compare the technical building blocks that are available at the moment and see how well they meet the regulatory requirements. (I2-T)

Such a process is described as this interviewee’s personal *modus operandi* for navigating PETs in the compliance sphere. If this process could be more universal, and accepted by the proper authorities, the utilization of PETs as technical measures could become more accessible and less “mysterious”.

It should be acknowledged that pursuits like the one described by S6 have been taken up by particular organizations. Particularly the IAPP, introduced in Chapter 3, make it a goal to disseminate this kind of material. Other resources, such as [89], provide great overviews of the technical side of the privacy discussion. Further work can definitely serve to harmonize more comprehensively both the technical and legal aspects involved here. Finally, supervisory and regulatory support is needed.

S7: Education

The promotion of education is something that can be viewed as crucial to the underlying “success” of privacy compliance going forward. The ultimate goal of starting at the educational level is to build up a strong foundation on the relevant material surrounding data privacy and its implications, such that the process of privacy compliance can proceed in a more informed manner and be supported more fundamentally. Where and how this can happen will be illuminated in part by the following.
The educational approach was first and foremost described in the interviews as happening in the industry, i.e. for those already finished with formal education. Although what exactly is needed by either more technically or legally oriented people was expressed slightly different, the overall premise is clear: “explain complex issues in a very simple manner” (I8-L). This complexity has certainly been a recurring theme, pertaining to the complicated dynamics, technologies, and driving factors behind the implementation of technical measures. A couple of interviewees hit upon this complexity that arises in their work.

On the technical side of things, education can help to reduce the perceived difficulty of implementing sound technical measures. For example with PETs, one interviewee sees the need to “reduce this complexity for the developer… if they want to use this technology, they should have some basic understanding of what that level is to achieve.” (I15-T). Clearly, if one wants to implement a PET, the basic understanding needs to be there. This sort of technical know-how is also desired from the legal side, as expressed here:

Anything that comes, anyone who can kind of give me an easy understandable information so I could understand how to ensure these technical security measures, or how to protect this privacy by design, it’s all very welcomed. (I8-L)

Specifically with technical education for people with legal background, this would need to be approached somewhat differently, involving once again cross-disciplinary interaction:

I would like to understand more, I wish I had more time to get into that, because it would also help my theoretical work better. So now I have to go to the tech guys, and say, come on, explain it to me as if I were three years old, so that I can explain it again to my clients as if they were two years old. (I11-L)

One can even begin to see how the positive trickle-down effect that better education can have, particularly how it can promote more informed guidance and counsel, thus allowing for more informed decisions regarding the compliance process.

The theme of education does not only need to be in regards with technology. Indeed, an arguably even more important aspect would be privacy education. This is something that would not only benefit privacy compliance, but also for creating more informed citizens in the age of data. For as [90] puts it, “A basic understanding of online privacy is essential to being an informed digital citizen, and therefore basic privacy education is becoming ever more necessary.” Furthermore, while formal educational curricula may be beginning to acknowledge the importance of data privacy, it has yet to yield “concrete content in the area”. Such a gap certainly extends to the industry, where an emphasis on the importance of privacy may be missing simply due to lack of educational programs on the matter. In the end, education on proper compliance can be rooted in education on the importance of digital privacy. I4-T certainly agrees with this, emphasizing the crucial nature of privacy education: “the same thing needs to happen with privacy. Otherwise, all the legal expertise in the world is not going to grow the field.”

How these educational programs would be structured is also very important. The general sentiment seems to point towards regular, continuous training that keeps up-to-date with the
ever-evolving landscape of privacy (compliance). One interviewee gladly shares some details of a well-working system inside this particular organization:

I know that there are people who are experts in it, they will offer trainings pretty much every week, like you just dropped in and learn about it. That’s you work on like a part time rotation project to actually implement it in a system. So it’s, it’s very available. (I4-T)

Here, the interviewee describes an educational program where domain experts will pass on their knowledge of the relevant technologies for those who wish to learn more. This type of learning would also definitely be promoted by another interview, who says “Of course, learning is always a good thing. Continuous learning? Yeah, what I see in practice is that for people, of course, learning takes time.” (I5-LT). Yet another interviewee, in talks about security training programs within the organizations, says:

I could also imagine privacy aspects could also have similar training. So yeah, so that is important information that is shared in this training. And then you have to pass some kind of tests that try to make sure that you have actually gone through the training material. (I6-T)

It can be seen that such education on privacy, PETs, and the like would most likely be welcomed; furthermore, some sound programs and ideas are already in place that could serve as suitable templates.

As a final note, the need for better education cannot be fully discussed without addressing the role of academia. I15-T expresses this in an eloquent way:

You cannot achieve this without their support or contribution also from a connecting point, so what I expect is so, in the academic world, they are the ones leading the Privacy-Enhancing Technologies that are expected to have local operations industry also provide more realistic solutions, because they are really like activists so they they really want to protect privacy.

And as the “activists”, the responsibility falls upon the academic community not only to develop these technologies, but also to promote privacy itself, or rather the motivation and purpose behind these technologies. This would no doubt need to be reflected in the curricula as well. Surely, a hefty yet worthy task for academia going forward.

**S8: Raising Awareness, Changing Culture**

*Once you have implemented the right technical measures, and you have done the organizational measures and the knowledge, the right knowledge spreads, then the three play together.* (I11-L)

The solution concept introduced here is one that addresses many of the challenges identified in this work, and it goes hand in hand with the topic of education as introduced by S7. Essentially, the need for awareness rests in the thought that without the proper attitude
towards privacy, good privacy compliance will be more difficult to achieve. Thus, to reiterate, the culture surrounding privacy compliance is almost as important to its success as the technical measures themselves; “It is even more important than just the technical.” (I15-T).

One can view this solution concept from a myriad of angles. For starters, “We need improvement from many aspects, firstly we need better education.” (I15-T). Continuing the discussion from S7, the first requirement is quite straightforward in its relevance to awareness, for it is through education that the importance (and a certain urgency) of privacy can be ingrained.

Moving more into the aspect of culture, it has hopefully become clear that the (organizational) culture around privacy compliance can significantly affect the approach towards the implementation of technical measures. It is at this juncture, then, that the “culture change” needs to take place. Several interviewees see it this way, as well. I3-L says,

If we want people in a company to do [the technical measures], we have to understand the organization of the culture of the corporation and change the culture of the organization or change behaviors within that existing culture.

Another interviewee looks specifically towards management for this shift, something that was addressed by C3.1:

The management, first they need to understand what’s they should interpret, interpret the law correctly, and then they should design decisions based on that.

(I15-T)

And finally, in response to the question of the best way to start to address some of the challenges discussed here, I1-T makes a lofty, but telling request, namely “[A "Time Machine"] would be the only way to start fixing it now, even though it would be a huge culture shift.” Although this may be a bit out of reach for the moment, the point is clear. The awareness necessary for sound privacy compliance is something that takes time, and furthermore, something that cannot simply be “demanded” without consideration of the cultural (also, literally) aspect of the matter.

So besides education, what can be done and what is needed? As always, some interviewees come to the rescue with useful insights. One interviewee stresses the need for good communication, saying “it’s just kind of pure communication. Of course, it’s just individual training, raising your level of expertise, and so on. So that also helps.” (I8-L). Another interviewee echoes this, and takes it one step further:

We need more transparency, more trust, more open communications, more active communications... being able to help like have that be understood with all of this. And I guess, I tend to think about this as, I talked about, like critical digital literacy. (I9-T)

As can be seen by these statements, the task of raising awareness is one that involves multiple dimensions, with concrete steps such as training and communication, but also the call for transparency, trust, and digital literacy. As such, the complexity of the matter is once again solidified.
Internally, more can be done to promote awareness. In one particular organization, a new and unique role is described:

> We have this great internal structure where each business area has a nominated person called the privacy champ... And they will be the person that has more of a privacy understanding compared to the rest of the team, and maybe raising that awareness, but they also teach us about their business area so that we can have those conversations. (I14-L)

Such a role almost serves as the in-house privacy advocate, also playing a key part in important decisions regarding compliance. Such advocates are also needed externally, particularly in the quest for more technical input. I4-T says, “Get more engineers into government. Get more people familiar with lawmaking and government into engineering. Because I don’t think they really cross pollinate.” By “government”, it is certainly also meant that the technical influence in regulation should become stronger.

The whole conversation surrounding awareness can at times seem rather abstract. At its core, such a notion is indeed abstract, yet its concrete implications for the field of privacy compliance are real, as promoted by the interviewees. With this, the discussion of the integral part played by awareness and cultural in combination with the implementation of technical measures will end here, at least for this thesis. The work should most certainly continue, though, not only in the investigation of the cultural aspect of compliance, but also research into how we can best acknowledge and address this going forward. As one interviewee formulates the challenge: “We have to change behavior. And the big, scary thing is, we don’t know how that thing’s gonna happen, or when it’s gonna happen.” (I3-L). We can almost certainly begin to try, though.

**S9: Privacy Tools**

The solution concept here arises out of the near unanimous agreement in the interviews that automation tools can certainly help in the process of privacy compliance. This undoubtedly pertains to the automation of the documentation and interactions required along the way. In addition, privacy tools with regards to the selection and utilization of Privacy-Enhancing Technologies would be particularly helpful. As one interviewee (privacy engineer) says, “in order to use [PETs], you probably need somebody else to put in a year or two of making a really simplified library for you to pull from.” (I4-T). This also addresses the challenge of complexity. In short, a call for more research and work into the creation of usable, scalable privacy tools would surely aid in the mitigation of technical challenges during the privacy compliance process.

**S10: Technical Framework**

The challenge arising from the lack of a universal technical framework for privacy compliance was discussed in C2.7, and accordingly, such a framework comprises solution concept S10. Ultimately, this framework would serve to help organizations “measure” their compliance,
something that “moves away from subjective criteria to a more formalized way of measuring things” (I7-L).

Inspiration that could guide the creation of this technical framework can be taken from currently accepted standards. One interviewee makes this clear:

The frameworks in general are helpful. So like in tech on its own, we’ve got ISO, which is one of the most respected ones, and you’ve got NIST. If a respected body like one of those tears come out with something with more of a technical framework for privacy? I think people would be a lot more on board. I think it’s that trust, being able to trust the organization for a quality framework. (I14-L)

In this vein, modern security standards can be studied as successful examples of how privacy frameworks could be constructed, of course keeping in mind the distinguishing characteristics of both notions (recall C4.6). The other important idea that is alluded to here is the need for this potential framework to be universal, or at least widely accepted. If this could be accomplished, a certain trust in the process would reasonably be established, which in turn could address any perceived inequalities in compliance demonstration. Thus, the framework in question should certainly take this into consideration. Above all, the relevant supervisory or regulatory authorities would play a key role in the promotion and adoption of the technical framework.

A technical framework for privacy compliance would undoubtedly be a step in the positive direction for privacy compliance. In particular, many of the challenges, directly related to technical measures as well as external factors, could be alleviated if a sound and fair framework were to exist. As one can surely perceive, the frequent use of modality in the discussion of this solution concept hints at the fact that there is much work to be done. Even so, the pursuit of a technical framework should merit future research attention, and its successful adoption would be a major accomplishment.

S11: KPIs

How do you measure [compliance], what are the KPIs? (I7-L)

A very interesting avenue for research, possibly one that should even prelude S10, is raised by the introductory quote here. In the talks for many of the challenges identified in this thesis, one can arguably trace back their roots to the interpretative and subjective nature of the whole privacy compliance process, whether it be expertise regarding technologies or value placed on data protection. In all of these discussions, a central question that can be posed is: subjective matters aside, how would one even begin to measure privacy compliance?

One promising solution would come with the usage of Key Performance Indicators (KPIs). A cursory overview provided by [91] states some of the basic functions of a good KPI:

- Provide objective evidence of progress towards achieving a desired result
- Measure what is intended to be measured to help inform better decision making
- Offer a comparison that gauges the degree of performance change over time
If a hypothetical KPI system would be established to accomplish exactly these, the process of privacy compliance would be benefited in two major ways: (1) objectivity, and (2) measurability (over time). This, woven into a technical framework, could significantly benefit privacy compliance programs (and possibly make them more efficient).

Another related research path comes with privacy metrics, such as in this previously mentioned work [80]. If these could in turn be filtered and modified into privacy compliance metrics, they could play a similar role as potential KPIs. Again, note the modality – nevertheless, challenging, yet worthwhile pursuits.

A final note of encouragement to this matter comes from an interviewee, which echoes a previous statement:

There’s certainly a lack of technical framework at the moment. So to be quite honest, if that’s the topic that you’re working on, keep working on it. Personally, I see that this is important in order to into to solve this problem. (I7-L)

S12: Guidance from Authorities

A kind of a bridge between the two areas, the legal and the IT, would be supervisory authorities, because they play a huge role in this... if they would put their resources also to getting together in a sense, providing more guidance on this, that would maybe also help. (I8-L)

The role of supervisory authorities in the whole picture of privacy compliance certainly came across as important, but nevertheless as an area that needs some improvement. Particularly when it comes to technical measures, these authorities could also help to address some challenges by taking a more active guiding role in the compliance process.

A first note of importance is the fact that regulatory authorities are there to help. On the other hand, they may currently be perceived negatively, or rather in fear due to the weight of potential fines that may be handed down. This is the wrong way to look at it, as one interviewee would claim, and the authorities are “actually there to help and support you” (I14-L).

As noted in the interviews and introduced in Chapter 3, some national authorities have already stepped up and begun to take on active duties to aid the privacy compliance process. For example, the UK (ICO) and France (CNIL) seem to be at the forefront. In Germany, the Standard Data Protection Model helps to translate the requirements posed by the GDPR into actionable steps for data protection in practice. One interviewee is a proponent of such a model: “I really like this approach, I think it’s very forward looking. And it’s the only way to go.” (I5-LT). In this light, perhaps the next step is for more national authorities to release such models, or better yet, for a international version to be created.

Another area where authorities have started to branch out is in the dissemination of information. At least in Germany, one interviewee sees that the level of communication stemming from such authorities is at least partly adequate:

The gap is not as big as many people see it and because the [regulatory authorities] interact pretty well with the BSI. And the information more or less is good that’s
sent out to the DPOs... Whether this information is coming to the companies, to the internal DPOs, we have to see. (I12-L)

Here, one can see a dynamic illustrated where regulatory bodies interact with national institutions, who then collaborate to pass down relevant information to the important DPO roles. The one potential gap in this picture is the manner in which this crucial information is spread to all the other involved parties in the privacy compliance structure. This naturally goes along with the education and awareness aspect.

The main area where improvement can be enacted, and particularly relevant to this thesis, is the guidance provided by authorities with regards to the implementation of technical measures. It is here where a definite lack is perceived. Simply stated, organizations “need guidance… it’s better from the data protection authorities.” (I15-T). This notion suggests that legal counsel can only go so far, and guidance from higher authorities plays a key complementary role. Two other interviewees make this need for technical guidance more concrete:

The data protection authorities are still happy with doing very foundational stuff to meet the requirements. And what I would love to see in the near future is that they set up in the evaluation of technical solutions. (I2-T)

If the data protection authorities would take the stand and say, listen, if you do that, that’s fine with us, right? Because then that would really push the technology and I think would also be good in terms of meeting the purpose of the whole thing. (I7-L)

Interestingly, guidance from authorities would not only aid in evaluating technical measures, but also potentially driving innovation forward, as organizations become better informed of the right technical measures for their data processing activities and can thereby invest in developing and implementing these technologies.

All in all, more guidance from the proper authorities would almost certainly add a much needed benefit to the implementation of technical measures for privacy compliance. It is because of this that a large responsibility befalls all supervisory data protection authorities, whether national or international, for as one interviewee puts it, “They really have a long to-do list, more clear regulations and obviously more guidance for the companies, for the market.” (I15-T). While this undoubtedly is easier said than done, the objective is clear.

S13: Audits

Although only explicitly mentioned by one interviewee, an interesting solution concept comes with the ordering of external audits to evaluate an organization’s privacy compliance. In short, this decision falls upon management, since “if the management is not truly convinced that something is wrong and something needs to be changed, you can always kind of order an external audit.” (I8-L). There are certainly many additional factors that would play in here, first and foremost the necessary awareness and prioritization on the management
level that would need to be present for the decision to even be considered. On top of this, one can argue that an audit is not guaranteed to fix or even find potential data protection issues, and the process itself comes down to an interpretive assessment. Furthermore, audits directly evaluate compliance, but the many other factors as introduced in Chapter 7 would not be addressed. Despite these considerations, audits can serve as great motivators for the proper demonstration of privacy compliance, both on the technical front as well as the raising awareness piece.

S14: More Collaboration

The final solution concept promotes cross-organizational collaboration, with the thought that exchange between peers regarding privacy compliance practices can boost perspective as well as motivation. In this way, S14 is arguably one of the more immediately actionable solution concepts, for the infrastructure is already there; now, it only remains for the “lines of communication” to be opened.

A few interviewees provide insight on the clear benefits that collaboration amongst peers can bring. One privacy engineer sees “constantly engaging with industry for different best practices” (I4-T) as a definite advantage. An active interaction with academia was also expressed, as made clear by the willingness to participate in the interview. Such exchange can be incredibly fruitful to gaining multiple perspectives on the matter, and this certainly pertains to the technology at hand.

Collaboration can also take the form of case studies into peer organizations, through the lens of success stories but also of lessons learned. This can be particularly helpful to management level roles in informing decisions regarding compliance programs:

Really training and explaining or presenting cases that, for example, other companies in a similar situation have suffered, for example breaches or having been issued fines and so on. So that kind of puts the whole situation in perspective, that kind of issue you can show to the management that we’re not living on an isolated island. (I8-L)

On this note, privacy compliance can better be viewed as a collective effort towards data protection, rather than an individual pursuit, i.e. “an isolated island”.

With the seemingly long, winding path towards privacy compliance – rife with webs of interaction, technological complexity, and other confounding factors – one of the best (and most effective) resources for an organization can naturally be a peer organization, who is “in the same boat”. One interviewee hints at this idea:

I think sometimes, maybe this needs to sort of collaborate more with people outside of your organization, just that there are still certain gray areas in the law. But being able to collaborate with like organizations and getting a better understanding together might be helpful. (I14-L)

Again, this points towards a more communal aspect of the whole matter. After all, the ultimate goal can be argued to be the same for everyone.
9. Solution Concepts

One saw in Chapter 6 the intricate, potentially incomplete, structure of privacy compliance, which without a doubt necessitates interesting and sometimes challenging interactions. With this in mind, the concept promoted by S14 would almost be to “stack” multiple of these structures side by side, adding another dimension of interactivity and exchange. It can be said that organizations like the IAPP have already begun to facilitate this collaboration; as usual, more work remains to be done.

9.3. Solution Concept - Challenge Mapping

Now that the solution concepts have been introduced, it may be useful to illustrate their potential applicability, i.e. which challenges each solution concept may serve to mitigate. This is done in the form of a mapping, which connects each solution concept (by code) to one or more of the challenges from Chapter 7 (again, by code). This is done in Figure 9.1.
9. Solution Concepts

Explanatory Notes

The corresponding codes can be found for the solution concepts in Table 9.1 and for the challenges in Appendix B, specifically in the consolidated challenge table (Table B.1).

It should firstly be noted that the mappings in Figure 9.1 represent the author’s best assessment of each solution concept’s strengths in relation to the applicable challenges. The mappings that are presented, therefore, are seen as the most suitable ones, and it is most certainly the case that some connections are missing. These are intentionally left out for the sake of readability. As many of the challenges are inter-related, even across categories, the complexity of such relationships was not attempted to be represented in the mapping. Deeper analysis can certainly be performed to represent better and more fully the true inter-relatedness. For now, the mapping presented, as well as the corresponding discussion in this and the previous chapters, serve as an preliminary attempt.

In order to somewhat save readability, the arrows in Figure 9.1 are colored to denote to which challenge category a particular individual mapping belongs.

One special case comes with S8 and S9, which are bound together. As alluded to before, these two go hand in hand, and therefore they share the same mapping. In truth, as just mentioned, many other inter-dependencies exist, but perhaps this one is the most apparent.

Finally, it can certainly be seen that not all challenges receive an incoming connection. This above all points to the fact that some of the challenges identified in this work simply do not have easy or even readily perceivable solutions. As it turns out, many of these unmapped challenges pertain in some way to financial matters, incentive, and the more “abstract” concepts. In addition, challenges regarding uniformity in the privacy compliance structure are not addressed. These are all undoubtedly tough questions to answer.

9.4. Survey Findings

The conclusion of this chapter will involve a brief analysis of the final survey question, which prompted participants to select which of the (included) solution concepts they believed to be useful and worthwhile. In addition, an open-ended response was left to allow for write-in solution concepts. The findings from this particular question are visualized and analyzed below.

9.4.1. Solution Concept Scoring

A “scoring” for the solution concepts is visualized in Figure 9.2. A radar chart was chosen as the method of visualization, so that all scores and their relative strengths can be illustrated. Firstly, a few notes. As indicated in Table 9.1, the first five solution concepts were not included in the survey due to timing (survey began before these concepts were identified), so they are not included in the evaluation. As such, only S6 to S14 are included.

As also can be seen in Figure 9.2, two solution concepts were broken down into sub-concepts, i.e. one concept becomes two. This decision was made due to the multi-faceted nature of these solution concepts, as the feeling was that the distinction should be presented
to the survey respondents. These distinctions very much follow the discussion that was led in the introduction of the respective solution concepts.

As a final note, at the time of the creation of the visualization, 23 total respondents had completed the survey. The final survey question presented a list of options mapping back to each solution concept, and the respondents were tasked with the following question, which is recreated below to match the options provided with their respective codes in Figure 9.2:

*I think the following would serve to mitigate some of the challenges existing within privacy compliance today:*

- [S6] Mapping of PETs to privacy regulation
- [S7−1] More / better educational materials about PETs
- [S7−2] More emphasis on privacy in our education systems
- [S8] General raising awareness about the importance of privacy (compliance)
- [S9] Better libraries for privacy tools
- [S10] A technical framework (e.g. specifications, standards) for privacy compliance
- [S11] Privacy compliance KPIs
- [S12−1] More guidance from supervisory / regulatory authorities
- [S12−2] More interaction with supervisory / regulatory authorities
- [S13] More audits
- [S14] More collaboration between peer organizations

The respondents could choose as many options, or none, as desired. In the end, the maximum number of times an option was selected was 15, which serves as the maximum “score”. Scores included firstly the percentage of respondents selecting the option, as well as the raw count. Accordingly, all scores are visualized in Figure 9.2.

It should be noted that some responses entered in the “Other” option included discussion fora, whistle-blowing support, education to the public, and more individualized liability.

**Analysis**

Observing Figure 9.2, one can see that the solution concepts regarding the needs for increased awareness and a technical framework received the highest scores. The interview insights would certainly agree with this, as these two concepts were quite often discussed in one way or another. Another confirming result comes with the relative high scores achieved by both S7 sub-concepts, both relating to the need for better education surrounding privacy and the appropriate technologies.

Surprisingly high results, i.e. ones that were not so emphasized in the interviews, came with the scores of S6 and S11. In the case of S6, the high score stresses the need for a stronger bridge between technologies developed to protect privacy and the regulations in place that also aim to do just that. If these two can be harmonized, the demonstration
of privacy compliance via technical measures can be better guided. S11 calls for privacy compliance KPIs, and this is without a doubt something that could be beneficial, especially in the objectivity they provide. As such, the need for future work on the development of these for privacy compliance is confirmed.

One can also see that some solution concepts fall a bit short in terms of support. Above all, more audits seemingly would not be backed by many privacy compliance proponents. In addition, better libraries for privacy tools also comes in with a low score. When one places these results in juxtaposition to some of the highest scorers, the emphasis on “intangibles” such as awareness and education clearly triumphs that of certain tangible solutions. Another important contrast comes with the large support for a technical framework for privacy compliance, rather than privacy tools.

Further analysis can certainly be performed using the results provided in Figure 9.2. Furthermore, the five solutions concepts not included in the survey should also be studied and verified in the future. Even beyond this, the difference between receiving support in a survey as a potential solution and the ability for these concepts actually to be realized must also be taken into consideration. In this way, the cursory analysis performed here is just that, and it calls for future in-depth research.
10. Discussion

In this penultimate chapter, a meta-analysis is performed, looking primarily at the major lessons learned, the inevitable shortcomings, and of course, paths for future research.

10.1. General Insights

In the conducting of the interviews, a true plethora of insights were provided by the interviewees. And once again, the author would like to express his heartfelt gratitude for this. Unfortunately, not every single insight was directly applicable to the research goals of this work; nevertheless, there are some general insights from in and around the interviews (and survey) that merit to be included here.

RE: GDPR

Although the goal of this thesis was to analyze the implementation of technical measures in general, the conversation quite naturally often fell back to a discussion about the GDPR. And this is understandable, as the motivation for “technical measures” stems directly out of the GDPR text. In these excursions, some valuable insights were gained that speak for the positive impact that the GDPR has had, as well as a couple of concerns that merit further thinking.

The first significant impact that the GDPR has had come with the attention it has drawn. In a relatively sudden manner (emphasis on relative), the need for privacy and data protection became tangible, more so than its former status as a “niche”. I8-L also describes this sort of wave: “Once GDPR came, it started to attract more attention. It was kind of a big explosion, everybody suddenly started to think about these issues.”

The challenge of perceived vagueness was also spun in a positive light, seen more in the light of a necessary adaptability. The difficulties arising out of this fact, therefore, are not a fault of the GDPR or the regulators behind it, but rather as a consequence of the way things are regarding privacy and all its complexity. Indeed, the mixed results to survey question A2.2.2 (see Table B.2) reflect the overall sentiment towards these privacy regulations. One interviewee dives into this a bit deeper:

With the GDPR, you can’t write concrete measures, specific measures in law, because the law from from the beginning to the end takes more than a year? All the technical things you wrote already are already out. And that’s why the GDPR has this clever reach to say, you have to use a technical standard of the time. I think that’s the only way you can handle this. (I12-L)
10. Discussion

One can certainly sympathize with this sentiment, and this circles back to the utmost interesting dynamic of the “foot race” between law and technology.

Seen in a more critical light, though, one may question as to whether the GDPR is truly a step in the right direction with regards to data privacy. Specifically, one interviewee is skeptic:

I think, in general, there’s the question of whether these regulations are the right thing... there needs to be a way of trying to get to that sort of root cause and rethink about like, what privacy is needed better. (I9-T)

One has hopefully seen how the desire for strong data protection has set off this journey of privacy compliance and technical measures, but one may wonder if the train has left the station and left privacy behind (recall C4.7). Even if this were true, what is the alternative to regulation?

Another large critique of regulations like GDPR revolves around one of the defining characteristics of these regulations: their (perhaps too) encompassing nature. Under the jurisdiction of the GDPR falls a veritable spectrum of organizations and entities, yet little to no distinction is made between them. As an interviewee puts it:

It would make sense to differentiate between company sizes of companies or business branches and so on. Right now, a five person web design agency has to fulfill the GDPR as well. And this is for them a problem. Not hard for [a large tech conglomerate]. (I12-L)

I10-LT also brought up the somewhat contrived (but apparently real-life) example of the data protection authorities demanding the appropriate technical measures to be taken by a local bakery (that must have been doing some form of data processing). Meanwhile, massive tech companies may have entire departments and dozens of employees dedicated to privacy compliance alone. The critique here is arguably justified, and it is an area where the GDPR may fall short as it stands.

Nevertheless, one cannot reasonably expect perfection from regulations like the GDPR, especially as they are still in relative infancy. Remarkably, in a few short years, the GDPR is already widely viewed as the “Golden Standard” for data protection regulation. In survey question A2.1.5, 22 respondents (95.7%) stated that they work with GDPR the most. Several interviewees also made a point of this:

GDPR in itself is a golden standard with data protection and privacy law... and that plays a crucial role. (I16-L)

The GDPR itself, the golden standard, a lot of these local laws, either have already been adapted to be basically copy-paste kind of on the way to be updated to comply with the requirements of GDPR. (I8-L)

Nowadays, it’s pretty easy, because once you’ve got GDPR handled, everybody else copies GDPR concepts. (I5-LT)
10. Discussion

It is definitely amazing to observe how similar sentiments were expressed from independent voices across the world. Indeed, GDPR’s impact is certainly far-reaching. This is also readily apparent in the way that many new regulations have sprung up worldwide that take clear inspiration from the GDPR. Specifically in 13 major nations, this effect can be traced directly back to the GDPR [92].

As a final note regarding the GDPR, its impact has soared far beyond the realm of legislation, and can arguably be seen as having influenced society on a much more foundational level. One insightful quote to this:

So I think that in these couple of years, the level of awareness and the level of compliance and such has just grown tremendously. . . And now it’s something that when you mention GDPR, anybody on the street will know what it is. (I8-L)

In this light, one also gains hope that we are simply still in the growing stages of privacy awareness, and that with time, the value of privacy (compliance) as it pertains to our society will become more and more commonplace.

The Good!

It is easier to be critical than correct.

– Benjamin Disraeli

With the rather lengthy discussion on the many identified challenges introduced in Chapter 7 and analyzed in Chapter 8, it may be interpreted that there exists widespread, systemic issues with the process of privacy compliance. This is in no way the intention of this work or of the author. Surely, there also exists a plethora of well-functioning and beneficial processes surrounding privacy compliance. The focus, however, is placed strongly on the challenges, i.e. where things may not be running so smoothly, for this is where attention should be drawn and improvement can be enacted.

It should be mentioned that many positive aspects of modern privacy compliance were mentioned in the interviews, and they therefore deserve an all-too-brief spot here. First and foremost, almost continuing the discussion from above, the requirement for privacy compliance has enforced a certain level of awareness for data privacy and data protection issues, regardless of whether people like it or not. The end result is positive: now more than ever, people across the world from a variety of organizations and cultures must look inwardly on their systems and processes in place and ask where privacy is at risk.

Out of this requirement for privacy compliance, one can clearly observe other positive outcomes. Specifically with technical measures, research interest for privacy and privacy technology has sharply risen (recall Figure 2.1). Surely, the current state of the research is arguably still in its adolescence, but one must start somewhere.

The coming together of all the different parties involved with privacy compliance can also be viewed in a positive light. Members from fundamentally different backgrounds, with the foremost example being technical and legal, now must work together on a regularly basis, whereas their interaction decades ago was nearly non-existent. Where challenges in
these interactions may exist, also exists the opportunity for overcoming these difficulties and forging strong, symbiotic, cross-disciplinary relationships.

Therefore, the “good” is without a doubt there. Only by placing emphasis on the “bad” and the “ugly”, though, one can take these positive aspects and make them better. While this discussion began in Chapter 9, it must certainly go on.

**Time is of the Essence**

In the conducting of the interviews and survey, an aspect that ended up playing a significant role, and one that was largely not considered in the planning of the thesis, was the timing. In short, one must consider the timing (time of the year, holidays, heavy work periods) of the prospective participants. While this might come across as self-evident, it especially plays a role when trying to coordinate across time zones and across the world.

Although the factor presented here did not ultimately hinder the completion of this thesis, it certainly necessitated careful rearrangement of planning and overlapping of work. As a possibly informative exercise, the interviews conducted over time are plotted as an accumulation in Figure 10.1, along with other important milestones of the thesis timeline.

![Accumulated Interviews Over Time](image)

**Figure 10.1.: Accumulated Interviews Over Time**

As can be seen from Figure 10.1, the accumulation of interviews was not immediate, only really picking up in late September. One sees here the possible effects of the summer months. In light of this, the thesis writing and survey creation needed to be overlapped precisely, such that enough information was collected to begin the process, yet while still allowing for new
insights from the later interviews. Ultimately, an important lesson learned is that for research that is heavily reliant on the participation of others, timing is of the essence.

10.2. Useful Findings

Along the journey of this thesis, several useful findings were discovered in the form of tools and processes, to which the completion of the work owes much. At the same time, other tools turned out to be not so helpful, and they are also mentioned below.

Transcription: Pros and Cons

Following a conducted interview, the process of transcribing the interview is one that required considerable time and careful attention. Most importantly, the usage of direct quotes as a primary source necessitates their accuracy. As a happy medium between efficiency and accuracy, the decision was made to utilize an automatic transcription service, namely otter.ai. Here, the pros and cons are discussed.

Certainly, the initial speedup of the transcription process afforded by Otter was clear. Provided one has an audio recording of the interview, the transcription takes no longer than 30 minutes. The result is a raw transcript, which is speaker-separated. In reality, though, the transcription software does not always get all of the words correct, and sometimes even speakers are mismatched. Nevertheless, an excellent starting point.

For each automatically-generated transcription, the next stage involved a cleaning process. This involved reading through the entire transcript, identifying points where clear errors (grammatical or word identification) were made. With the Otter UI, these points can be edited with the help of parallel audio playback of the particular point in the interview. As a general note, Otter most often made errors where the audio was a bit unclear, specific terminology and/or abbreviations were used, or where an accent was present.

After the transcript was satisfactorily cleaned up, it was exported to text and PDF format, both for posterity and for the qualitative data analysis, discussed next. In the end, a hybrid approach to the transcription process worked best, which was without a doubt enabled by the availability of services such as Otter. In terms of time commitment, it was not measured whether this approach or a purely manual approach actually sums up to the least amount of time – this would be quite interesting to know.

Qualitative Data Analysis: MAXQDA?

With the interview transcripts in hand, the next major step was to perform a qualitative data analysis, as described in Chapter 4. The main goal of this was to identify overarching themes

1Otter Voice Meeting Notes, https://otter.ai/
in the interviews, primarily in the form of challenges. As with the transcription, the initial thought was to make use of available automation tools to assist with this process. After some cursory research, MAXQDA [39] was selected as the tool of choice. Above all, it was chosen due to its promoted automation of the coding and analysis of qualitative data, precisely what was needed (or perhaps not).

The major challenge with the use of MAXQDA comes with ability to analyze texts at a deeper semantic level. On the surface, the program contains very good tools to analyze and visualize characteristics of a set of documents, such as word frequencies, lemmas, etc. This, however, was not required for this thesis.

In order to “code” the set of transcripts according to challenges, one must manually create a dictionary in the program, which defines each desired category, as well as the corresponding key words and phrases for each. The main limitation with this, though, is that the identification of challenges from the interviews does not come in a standard format, i.e. the challenges will not always be phrased in the same way. As a result, the creation of such a dictionary is quite difficult to do in a comprehensive way. An example of the management of these dictionaries is given in Figure 10.3 (source: [93]). If the key words and phrases are chosen to be too general, then the transcripts are coded too generously, resulting in non-helpful coded documents. If too specific formulations are entered, then general themes cannot be identified.

For these reasons, the use of MAXQDA was abandoned and replaced by a completely manual method, which is outlined next. It must be stated that for certain use cases, MAXQDA can undoubtedly serve as an extremely helpful tool, especially for the resulting visualizations. Unfortunately, this was not the case here.

![Figure 10.3.: MAXQDA Dictionary in Action](image)

**Working with Quotes**

In lieu of an automated method for performing the qualitative data analysis, a manual method was followed, using the guidelines as discussed in Chapter 4 as a basis. In the end, the
process can be summarized as the following:

- As each transcript becomes available:
  1. Re-read the transcript
  2. Highlight excerpts of noted importance or significance

- Once all transcripts are processed:
  1. Assign each excerpt to a particular theme (structure, challenge, solution concept)
  2. Codify and consolidate until themes are distinct

The result of this process yields annotated transcripts and a codified table of excerpts (quotes), which are mapped back to the transcripts (by page). An abridged version of the resulting code map can be found in Table 10.1.

<table>
<thead>
<tr>
<th>Code / Topic</th>
<th>Interviewee</th>
<th>Quote</th>
<th>REF_PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPO</td>
<td>I2-T</td>
<td>At the end of the day, the data protection officer is more a legal person than a technical person.</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>I3-L</td>
<td>There are de facto go-betweens. And those are usually in the compliance office.</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>I5-LT</td>
<td>The person taking care of data protection in an organization needs to be hybrid. In my case, that’s me.</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>I6-T</td>
<td>They have their own data protection team and that team has multiple members and when the project is being set up, you contact the team and they locate at least one person for for that specific project.</td>
<td>154</td>
</tr>
<tr>
<td></td>
<td>I6-T</td>
<td>The data protection team definitely has lawyers working there.</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>C1.7</td>
<td>I5-LT</td>
<td>But we need we need these guys to talk to the IT department. And that needs to be in the same place.</td>
<td>84</td>
</tr>
<tr>
<td></td>
<td>I8-L</td>
<td>The main point would be just communication between the teams, the legal team to really understand what the IT team has, for the IT team to understand what are the legal requirements, because I think that is where there’s a lack of communication.</td>
<td>115</td>
</tr>
<tr>
<td></td>
<td>I9-T</td>
<td>I think it requires like cross communication and processes to a large point…And this goes to that, like organizational culture. [+ 3.2]</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>I16-L</td>
<td>That is the most important part as far as privacy compliance is required because both things, the tech and legal thing goes hand in hand to privacy compliance.… it is very rare to find, but it would be very ideal if tech and legal worked side to side.</td>
<td>233</td>
</tr>
<tr>
<td>Certification</td>
<td>I2-T</td>
<td>It helps you to better read the law and interpret the law and also to better create things like statements for consent</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>I7-L</td>
<td>I think [greater technical input] will become standard with certification schemes.</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>I16-L</td>
<td>The primary education for these tools are from the certification and the courses which we do and the teammates are certified.</td>
<td>228</td>
</tr>
</tbody>
</table>

Table 10.1.: Qualitative Data Analysis Codified Table, Abridged
10. Discussion

As a note, the REF_PAGE columns refers to the page number in the complete merged transcript document, such that all page numbers are unique. With this completed table, the interviews as a whole can be summarized, which greatly aided in the writing of this thesis. Therefore, such a methodology proved to be quite useful, particularly since these quotes drive many of the discussions carried throughout the work.

draw.io, excellent

As another useful finding, draw.io\textsuperscript{2} was (re)discovered as an excellent tool to create all sorts of visualizations. In particular, the diagrams of Figures 6.1 and 9.1 were created using this tool. For a free-to-use tool, draw.io serves as an excellent resource for putting together an extensive variety of visualizations – kudos to the creators.

Who You Know + Making Things Interesting

A final useful finding, perhaps one that needs no mention, is the value of personal connections in the search for interview and survey participants. In addition to reaching out to newly found contacts, second-degree connections also proved to be highly respondent.

Along these lines, much was learned about incentivizing participation in the absence of traditional incentives, e.g. a financial one. Personalizing messages and doing so succinctly certainly helped to a degree. Particularly with the survey, much work needed to be invested into finding willing respondents beyond the original interviewee participants. By expending various channels, this was slowly yet surely accomplished (see limitations below). In the end, one helpful step proved to be the creation of an eye-catching graphic to go along with the appeal for participation. This is presented in Figure 10.4, if for nothing else to bring in a little color to round out this section.

\textbf{Figure 10.4.: Call for Survey Participants}

\textsuperscript{2}Flowchart Maker & Online Diagram Software, https://app.diagrams.net/
10. Discussion

10.3. Perceived Limitations

The work performed in the scope of this thesis certainly did not come without its limitations. While it cannot be said that these limitations hindered the completion of the thesis, they represent areas that could have ultimately further improved the research results, had the limitations not been there. The limitations discussed below are included to acknowledge the inevitably bounded scope of this thesis, serving as a precursor to areas of future work, covered subsequently.

Interviewee Pool

The number of interviewees who contributed to this research work is seen by the author to be quite adequate. The limitation, though, comes with the diversity of the pool, particularly in the geographical aspect. As illustrated in Chapter 5, the geographical diversity is decently rich, spanning multiple continents. However, one can see clear gaps. The South American and African continents were completely left out, as well as major parts of Asia. Although one could argue that this is very telling of the privacy compliance landscape of today, it would have nevertheless been worthwhile to hear from the voices working out of these regions.

Among the interviewees, it would have also been interesting to hear from some different roles, such as some of those included in Figure 6.1. Fortunately, the function of many of these roles within the privacy compliance structure was learned secondhand via other interviewees. Nevertheless, conversing with some of these other roles in person could have undoubtedly enriched the overall picture, as well as potentially uncovered additional challenges and solution concepts.

The limitation here expresses somewhat wishful thinking, and one must not neglect the fact that the interviewees that did participate already represent a diverse, knowledgeable group of professionals who expertly provided rich insights. As such, these results would be well served to be expanded upon by new voices, for as the saying goes: the more the merrier.

Survey Responses

As already alluded to, the quest to find qualified, motivated, and willing survey participants proved to be quite challenging, even relative to the search for interviewees. Starkly in contrast to the original idea that surveys would present a much more convenient, and thereby accessible, form of research participation, the process required a multi-front effort from several people in addition to the author.

With this said, the final number of respondents is perceived to be acceptable. After all, the type of person who could confidently answer the full survey is still relatively rare, in comparison to other established forms of compliance, or other related processes. It is nevertheless a sure thing that more responses would lend a greater confidence (and possibly diversity) to the survey findings. One silver lining is that there is no established “minimum amount” of responses to validate the findings; furthermore, arguably more important is the analysis and insights that can be extrapolated from what was achievable. In this light, the
findings as they stand may be seen as an exploratory probe into the matter, with the call for wider, more encompassing studies to follow.

10.4. Future Work

In the consideration of how to present avenues for future research in a clear and concise manner, it was decided to do so along the lines of the four challenge categories presented in this work. This can serve to provide some structure to the discussion, as well as allow for the distinct separation and itemization of future work.

Technical-Legal Interaction

- Bridging the Gap – how can we better understand and harmonize the technical and legal mindsets?
- Interaction in Practice – deeper (case) studies into how this interaction unfolds in day to day work
- Building Cross-Functional Teams – how would these be comprised, is it feasible, what would be the designated roles within for privacy compliance?

Technologies

- PETs Education – more work on making PETs more accessible and learn-able, not just for technical experts
- PETs + Regulation – how do PETs fit in (and map to) modern privacy regulations and their requirements?
- Technical Framework – implementable framework for technical measures
- Resources – what is the true “cost”, complexity, and infrastructure needed to implement privacy technologies?

Organizational Factors

- Organizational Culture – in-depth studies of organizational culture and the role of management, as it pertains to data privacy (compliance)
- Privacy Compliance Structure – validate, revise, and refine the structure as proposed in Chapter 6 and Figure 6.1
- Technical Measures – what these mean to different organizations, considering the many different factors at play
10. Discussion

General

• Inequality in Privacy Compliance – does this really exist / is perceived? If so, where does the problem lie?

• The Meaning of Privacy – what does privacy mean to people, on a technical, legal, sociological, philosophical, or otherwise relevant level?

• Privacy in Regulation – how do legal requirements for privacy, data protection, etc. align with what people believe to be at risk?

As a final category for future work, the challenges and solution concepts introduced in this thesis can all serve as the basis for new research questions. Above all, their validity and relevance are open to further analysis (and possibly even refutation!). As mentioned near the beginning of this work, the ultimate goal of this thesis is to start the discussion – validation, revisions, and criticisms are all very much welcomed.
11. Conclusion

In a time where data abounds, its power has been realized through the development and improvement of a myriad of new technologies and services. This has pervaded modern day thinking to the point where innovation has almost become synonymous with, or perhaps even necessitated by, data processing activities. At the same time, an increasing concern for the protection of privacy has ignited a newfound interest in data privacy, as well as the search for how best to protect it. The adoption of data protection regulations, underpinned by the employment of technical measures to safeguard privacy, has stepped to the forefront of these efforts, with the primary goal of enforcing responsible data processing practices, achieved through the idea of compliance.

Firstly looking beyond the sphere of regulation and compliance, one comes to realize that the study of privacy illuminates a unique and intriguing history. This certainly predates the notion of “big data”; nevertheless, the focus on how the usage of data can be reconciled with privacy has brought a whole new dimension to the matter. With the introduction of new technologies designed to preserve privacy, mixed in with the ecosystem of privacy and data protection regulations, the waters can become a bit muddied.

Beginning the investigation of the role of technical measures for privacy compliance, one learns that the compliance process involves an intricate web of roles, responsibilities, and interactions. At the core of this structure lies the coming together of the technical and legal sectors, something which comprised a key area of focus for this thesis. Chapter 6 explored this privacy compliance structure at a generalized level, uncovering some of the crucial sub-processes and interactions that must take place in order to realize technical measures for privacy compliance.

Indeed, the highly complex machine that is the privacy compliance structure is sure to possess some inefficiencies, particularly as it is still in relative infancy (in the modern sense). This served as the major hypothesis of this work, and Chapter 7 aimed to identify and analyze a number of challenges uncovered via the expert interviews. In total, 33 distinct challenges were identified, all pertaining in some way to the implementation of technical measures for privacy compliance. Admittedly, while some of these challenges are clearly directly related, others hit at the matter in more subtle, or rather intangible, ways. Furthermore, the inter-relatedness of many of the challenges also showcase their inherent complexity. In this light, the challenges were divided into four categories, pertaining to either the Technical-Legal Interaction, Technologies, Organizational Factors, or General Concepts. Together, these challenges form the heart of the investigation, pointing to areas of the privacy compliance process that require future attention and present opportunities for improvement.

The discussion of the identified challenges would not be considered complete without at least a cursory exploration into possible solutions. This became the goal of Chapter 9, which
11. Conclusion

introduced 14 solution concepts, defined as ways in which some of the identified challenges can potentially be mitigated. These solution concepts can map to one or many of the challenges, highlighting their versatility as well as once again displaying the inter-relatedness of the challenges.

Through the use of a mixed-method approach, the ideas, challenges, and solutions extracted from a qualitative analysis could be further studied and preliminarily verified via a quantitative analysis. Thus, the main goal of Chapter 8 and the latter part of Chapter 9 became to perform this analysis, with the aid of the survey results. A particular emphasis is placed on the preliminary nature of these analyses, and they would be well-served to be further expanded upon in the future.

In a similar light, the crux of this thesis is to investigate potential challenges in what is believed to be a very important field, especially going forward. Specifically, the use of technology to meet the requirements of privacy regulations, and furthermore to achieve true data privacy in the best way possible, is viewed as a noble pursuit as well as one demanding further work. As such, the work performed here is primarily meant to start the discussion. The challenges introduced in this thesis can most certainly serve as starting points for novel research, and at the very least, represent the seeds for more in-depth investigation and debate. This is the author’s main intent, and the prospect of improving such an important (and young) field is truly exciting.

Thus, the work of this thesis concludes here, but the work surrounding it can (and should) without a doubt continue. Now more than ever, we are spiralling towards a realm where data is king, but the question of how to best ensure its responsible and ethical use remains in the hands of researchers, privacy professionals, and data privacy proponents alike. Surely, challenges exist (and presumably always will), but through the continual identification and mitigation of these, the process will only become stronger and more resilient. For it is only through such endeavors that personal privacy can be protected, in an age where it is increasingly endangered.

Privacy is not something that I’m merely entitled to, it’s an absolute prerequisite.

– Marlon Brando

– SJM, 05.01.2022
A. General Addenda

A.1. Interview Questionnaires

The interview questionnaires used in both the technical and legal interviews are included below. To give the reader a better sense of the format, the original documents (i.e. the ones sent to the interviewees and followed during the interviews) are inserted.
Interview Questionnaire (Technical)
Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance

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?

Background
1. What is your position and role?
2. How many years of experience in this field and in the company do you have?
3. What is the size of your team? How many teams are you responsible for? Where are the team members located?
4. Generally speaking, how would you define privacy? Privacy compliance?
5. What are the software systems that you are developing/maintaining? Is privacy at risk?
6. With which privacy regulations are you required to be compliant?

Privacy Regulation Identification
7. What is your understanding of the “technical measures” required to comply with privacy regulations?
8. How do you process and implement privacy regulations in your work? Do you have a structured procedure for privacy compliance (e.g. guidelines)?
9. How do you ensure the system is complying with the legal requirements?
10. What are the main artefacts (documents, diagrams, etc.) that you use in the process of privacy engineering?

Privacy Requirements and Liability
11. With whom do you directly interact when it comes to privacy engineering?
12. What are the main roles/positions in your team/department/company responsible for the implementation of privacy requirements?
13. Are there any external stakeholders in the process of privacy engineering (external legal experts, regulatory bodies)?
14. How do different stakeholders interact/communicate within the privacy engineering process?
15. Who is liable for privacy compliance?
16. In general, do you wish for better interaction with the legal support with respect to privacy questions or discussions? Is this necessary in your opinion?

Privacy Tools
17. What tools do you utilize for privacy engineering?
18. What was your experience in the use of these tools?
19. Do you use any Privacy-Enhancing Technologies (PETs) to achieve privacy compliance?
   19.1. If yes, which ones? How are these technologies introduced and taught to you / your team?
      19.1.1. Are there specific educational materials for the PETs?
      19.1.2. In what way can this process be improved?
A. General Addenda

A.1.2. Technical Questionnaire

19.2. If not, has the possibility been discussed?
   19.2.1. Would specific materials and/or courses relating to PETs be helpful tools?
20. In which parts of the compliance process could automation be applied in a beneficial way?

Legal Specification
21. How familiar are you with the privacy requirements that you need to adhere to during the design of software systems for / with which you are responsible / involved?
22. Who supports you with the understanding of the legal details required for the implementation of privacy requirements?
23. How do you interact with the legal experts involved in the process?
24. What specific information from legal experts do you need to make informed decisions about privacy compliance?
25. Could you describe an experience of working with a legal (privacy) expert? How strong was the mutual understanding regarding privacy compliance?
26. Does your organization utilize Data Protection Impact Assessments (DPIAs)? If so, how does this work? If not, has the possibility been brought up?

Looking Forward
27. Have you seen the process of privacy compliance develop and/or change with the introduction of new privacy regulations?
28. What has been the most challenging experience regarding privacy compliance?
29. In your opinion, what are the main challenges and barriers to the implementation of technical measures for privacy compliance?
30. How can these challenges and barriers be best overcome? Who should be responsible for this?
31. How can this process be improved or optimized from your perspective? What can be helpful in this process?
32. Do you feel that there is a need for better interaction between the technical and legal sides of privacy compliance?
33. Do you think that continuous learning with regards to this subject would be beneficial to you and/or your team?
   33.1. If yes, what you would like to see covered in these learning materials?
   33.2. What medium would be the most helpful?
34. Is there some other aspect to discuss that we may have missed?
35. Can you refer anyone else, either in the legal or technical fields, who could provide further insight into this research?
A. General Addenda

A.1.3. Legal Questionnaire

Interview Questionnaire (Legal)
Identifying Practical Challenges in the Implementation of Technical Measures for Data Privacy Compliance

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?

Background:
1. What is your position and role?
2. How many years of experience in this field and in the company do you have?
3. What is the size of your team? How many teams are you responsible for? Where are the team members located?
4. Generally speaking, how would you define privacy? Privacy compliance?
5. Which privacy regulations do you work with regularly / are particularly relevant to your work?

Privacy Regulation Identification:
6. What is your understanding of the “technical measures” required to comply with privacy regulations?
7. How do you process and implement privacy regulations in your work? Do you have a structured procedure for privacy compliance (e.g. guidelines)?
8. What are the main artefacts (documents, diagrams, etc.) that you use with regards to privacy compliance?

Privacy Tools
9. In what way, if any, are automation tools used in your work with privacy regulations?
10. What was your experience in the use of these tools?
11. Are you familiar with any Privacy-Enhancing Technologies (PETs) to achieve privacy compliance?
   11.1. If yes, how often do you work with these?
       11.1.1. How are these technologies introduced and taught to you / your team?
       11.2. If not, would specific materials and/or courses relating to PETs be helpful tools?

Technical Specification
12. How familiar are you with the technical implementations in software systems that are put into place to adhere to privacy regulation?
13. (How) do you interact with any technical experts (i.e. with the technical measures) involved in the process?
   13.1. If applicable, with whom do you communicate?
14. What specific information from technical experts would be beneficial to you in better understanding the implementation technical measures for privacy compliance?
15. Could you describe an experience of working with a technical (privacy) expert? How strong was the mutual understanding regarding privacy compliance?
16. In what way, if any, is your organization involved with the process of carrying out Data Protection Impact Assessments (DPIAs)?
Looking Forward:
17. Have you seen the process of privacy compliance develop and/or change with the introduction of new privacy regulations?
18. What has been the most challenging experience regarding privacy compliance?
19. In your opinion, what are the main challenges and barriers to the implementation of technical measures for privacy compliance?
20. How can these challenges and barriers be best overcome? Who should be responsible for this?
21. How can this process be improved or optimized from your perspective? What can be helpful in this process?
22. Do you feel that there is a need for better interaction between the technical and legal sides of privacy compliance?
23. Do you think that continuous learning with regards to this subject would be beneficial to you and/or your team?
   23.1. If yes, what you would like to see covered in these learning materials?
   23.2. What medium would be the most helpful?
24. Is there some other aspect to discuss that we may have missed?
25. Can you refer anyone else, either in the legal or technical fields, who could provide further insight into this research?
A. General Addenda

A.2. Survey Questions

Unless otherwise noted (with a *), the response options to the following questions follow the Likert-scale, as discussed in Chapter 4. In addition, responding to certain statements sometimes only makes sense if the response to a previous question was answered in the affirmative. Therefore, questions / statements with a “N/A” option are marked with a †. Note that only the survey questions / statements are provided here, except in the case of the “Looking Forwards: Solution Concepts” section. For a full copy of the administered survey, please view this link.

A.2.1. Background

1. What is your current role / position?*
2. How long have you been working in the privacy field?*
3. How large (roughly) is your current company / organization?*
4. Do you work in a team?*
5. Which privacy regulations do you interact with the most?*
6. Do you work more on the technical or legal side?*

A.2.2. Challenges: Technical-Legal Interaction

Note that in this section, slightly different statements were provided depending on the answer to the last question of the Background section. These differences are denoted by brackets.

1. I am quite familiar with the privacy regulations that are pertinent to my work.
2. These regulations are largely easy to understand and comprehend.
3. I rarely interact with more [technically-|legally-]oriented people regarding privacy compliance.
4. When interacting with [technical|legal] experts about privacy matters, the process can be slow or frustrating.†
5. When interacting with [technical|legal] experts about privacy matters, I feel like there is a disconnect that creates challenges.†
6. I believe there is a need for more and/or better interaction between the technical and legal sides of privacy compliance.
7. I believe that in general, there is a lack of [technical|legal] knowledge on the [legal|technical] side.
8. Data privacy and privacy compliance are becoming more and more technically-centered.
9. There is a need for more technically-minded people in the conversation about privacy compliance.
10. Any perceived gap in knowledge or understanding between the technical and legal sides of privacy compliance is a good thing.

11. There is a lack of interdisciplinary / cross-functional teams in privacy compliance programs, i.e. a better balance is needed.

12. As a technically-oriented person, I feel like the makeup of current privacy regulations leaves much of the interpretation work up to me.

13. I believe my answer to the question above is the optimal state of things.

A.2.3. Challenges: Technologies

1. My regular work with privacy compliance makes use of automation tools.

2. I am familiar with the concept of Privacy-Enhancing Technologies (PETs).

3. PETs are among some of the best current methods for being compliant to privacy regulations (regarding the "technical measures").

4. I feel like there is a lack of proper characterization of PETs (how they work, benefits, disadvantages, etc.).†

5. PETs are actually quite difficult to implement in practice.†

6. The ability to implement PETs is very dependent on a company’s resources.†

7. In general, the understanding of PETs requires a sound technical baseline.†

8. Communicating about these PETs with people with purely legal background is quite difficult.†

9. There is no clear sense of how PETs relate to privacy regulations.†

10. I believe there is a general need for better education on PETs.†

11. I personally am interested in learning more about PETs.†

12. Specifically, I would like to learn more about PETs regarding . . . †

13. There is a general lack of technical literacy when it comes to privacy compliance.

14. There does not exist a solid technical framework for privacy compliance.

15. I believe there is little incentive to put resources into implementing the newest, state-of-the-art Privacy-Enhancing Technologies.

16. It is more convenient and/or economical not to put time and resources into implementing sound technical measures.

17. I believe that there are many technologies for data protection, yet the awareness and knowledge surrounding them is lacking.

18. Privacy compliance doesn’t motivate the innovation of technology in the privacy field.
A. General Addenda

A.2.4. Challenges: Organizational

1. I have an established point of contact in the case I have questions or concerns regarding privacy compliance.
2. I regularly interact with a Data Protection Officer or similar role.
3. If not DPO, please name role:*†
4. When it comes to interpreting privacy regulations, this interpretation comes from the management level within my organization.
5. I believe there are many ways to approach privacy compliance, specifically regarding technical measures.
6. There is an inequality in the current industry as to what suffices as "being compliant".
7. The politics within an organization may affect the degree to which sound technical measures are pursued.
8. My organization has an established and easy to understand structure with respect to privacy compliance.
9. I believe this structure matches that of peer organizations within my field.†
10. More focus should be placed on "privacy engineering" within organizations.
11. On the whole, I would say legal support is readily available to me regarding any privacy-related matters.
12. The implementation of technical measures for privacy compliance can be challenging depending on what systems are involved.
13. Privacy compliance can be a bit of a "gray area".
14. When it comes to technical measures for privacy compliance, this largely becomes a financial matter (creates a significant overhead).
15. Demonstrating sound privacy compliance can actually boost a company’s value.
16. At the core of implementing technical measures for privacy compliance is a risk assessment, which is dependent on organizational culture.

A.2.5. Challenges: General

1. I believe that the amount of privacy regulations nowadays makes implementing technical measures for privacy compliance convoluted.
2. There is a clear need for better "harmonization" of these regulations (and requirements).
3. Privacy compliance involves too much bureaucracy.
4. All in all, I think recent years have seen the industrialization of privacy (compliance). With ‘industrialization’ is meant the transition from a "niche" profession to a more product and revenue driven industry.
5. This industrialization is in my view a positive advancement.†
6. It is often the case with privacy compliance that although compliance can be argued for, true protection of privacy may not be achieved.

7. There is such a thing as "over-compliance".

8. In general, I think the concept of privacy itself is quite vague or not well-defined.

9. The meaning of privacy is distinct from, and often conflated with, the concept of data protection.

10. Being 100% compliant does not imply 100% data protection.

11. The true meaning of privacy has been lost in modern privacy compliance.

A.2.6. Looking Forwards: Solution Concepts

I think the following would serve to mitigate some of the challenges existing within privacy compliance today:*  

• Mapping of PETs to privacy regulation  
• More / better educational materials about PETs  
• General raising awareness about the importance of privacy (compliance)  
• More emphasis on privacy in our education systems  
• Better libraries for privacy tools  
• A sound technical framework (e.g. specifications, standards) for privacy compliance  
• Privacy compliance KPIs  
• More guidance from supervisory / regulatory authorities  
• More interaction with supervisory / regulatory authorities  
• More audits  
• More collaboration between peer organizations  
• Other

A.3. Survey Link

A link to the closed survey (Google Forms) can be found at: https://forms.gle/eMRTu9nvxSnB2UWt9.
### B. Figures and Tables

#### B.1. Complete Challenge Table

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1.1</td>
<td>Rare direct interaction with legal</td>
</tr>
<tr>
<td>C1.2</td>
<td>Interaction with legal is frustrating / not desired</td>
</tr>
<tr>
<td>C1.3</td>
<td>Deadlock between technical and legal mindsets</td>
</tr>
<tr>
<td>C1.4</td>
<td>Technical knowledge lacking on the legal side, and vice versa</td>
</tr>
<tr>
<td>C1.5</td>
<td>Lack of technical input in privacy compliance</td>
</tr>
<tr>
<td>C1.6</td>
<td>Technical-legal gap is desired</td>
</tr>
<tr>
<td>C1.7</td>
<td>Lack of interdisciplinary / cross-functional teams</td>
</tr>
<tr>
<td>C2.1</td>
<td>Lack of a proper characterization of PETs</td>
</tr>
<tr>
<td>C2.2</td>
<td>Level of implementation depends on a company’s resources</td>
</tr>
<tr>
<td>C2.3</td>
<td>Difficult to communicate PETs</td>
</tr>
<tr>
<td>C2.4</td>
<td>No mapping of PETs to regulations</td>
</tr>
<tr>
<td>C2.5</td>
<td>Need for better education on PETs</td>
</tr>
<tr>
<td>C2.6</td>
<td>Lack of technical literacy</td>
</tr>
<tr>
<td>C2.7</td>
<td>Lack of a technical framework for compliance</td>
</tr>
<tr>
<td>C2.8</td>
<td>Companies implementing PETs are not rewarded</td>
</tr>
<tr>
<td>C2.9</td>
<td>The technologies are there, but the awareness isn’t</td>
</tr>
<tr>
<td>C2.10</td>
<td>Privacy compliance doesn’t motivate the innovation of technology</td>
</tr>
<tr>
<td>C3.1</td>
<td>It is often up to management to make decisions regarding regulations</td>
</tr>
<tr>
<td>C3.2</td>
<td>Organizational culture or politics have implications on technical measures</td>
</tr>
<tr>
<td>C3.3</td>
<td>Lack of uniformly defined roles</td>
</tr>
<tr>
<td>C3.4</td>
<td>Not enough focus on privacy engineering</td>
</tr>
<tr>
<td>C3.5</td>
<td>Availability of legal / supervisory support differs by company</td>
</tr>
<tr>
<td>C3.6</td>
<td>Technical measures are difficult for certain organizations</td>
</tr>
<tr>
<td>C3.7</td>
<td>Technical measures for privacy compliance is a financial concern</td>
</tr>
<tr>
<td>C3.8</td>
<td>Technical measures depend on a risk assessment, which can vary</td>
</tr>
<tr>
<td>C4.1</td>
<td>The amount of regulation (and &quot;settings&quot;) makes technical measures complicated</td>
</tr>
<tr>
<td>C4.2</td>
<td>Bureaucracy is a huge challenge</td>
</tr>
<tr>
<td>C4.3</td>
<td>Industrialization of privacy</td>
</tr>
<tr>
<td>C4.4</td>
<td>&quot;Bare minimum&quot; technical measures / inequality</td>
</tr>
<tr>
<td>C4.5</td>
<td>Privacy itself is difficult to understand or define</td>
</tr>
<tr>
<td>C4.6</td>
<td>Privacy is often conflated with data protection / security</td>
</tr>
<tr>
<td>C4.7</td>
<td>The true meaning of privacy has been lost in modern privacy compliance</td>
</tr>
</tbody>
</table>

Table B.1.: The Complete Coded Challenge Table
B.2. Complete Survey Results

<table>
<thead>
<tr>
<th>Question</th>
<th>%</th>
<th>Yes</th>
<th>No</th>
<th>Don't Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2.2.1 I am quite familiar with the privacy regulations that are pertinent to my work.</td>
<td>10</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>A2.2.2 In general, privacy regulations are easy to understand and comprehend.</td>
<td>3</td>
<td>4</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>A2.2.3 I rarely interact with more [technically] [legally]-oriented people regarding privacy compliance.</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>A2.2.4 When interacting with [technical] [legal] experts about privacy matters, the process can be slow or frustrating.</td>
<td>2</td>
<td>3</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>A2.2.5 When interacting with [technical] [legal] experts about privacy matters, I feel like there is a disconnect that creates challenges.</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>A2.2.6 I believe there is a need for more and/or better interaction between the technical and legal sides of privacy compliance.</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.7 I believe that in general, there is a lack of [technical] [legal] knowledge on the [legal] [technical] side.</td>
<td>12</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.8 Data privacy and privacy compliance are becoming more and more technically-oriented.</td>
<td>4</td>
<td>12</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.9 There is a need for more technically-minded people in the conversation about privacy compliance.</td>
<td>5</td>
<td>12</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.10 Any perceived gap in knowledge or understanding between the technical and legal sides of privacy compliance is a good thing.</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>A2.2.11 There is a lack of interdisciplinary / cross-functional teams in privacy compliance programs, i.e. a better balance is needed.</td>
<td>6</td>
<td>11</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>A2.2.12 As a [technically] [legally]-oriented person, I feel like the makeup of current privacy regulations leaves much of the interpretation work up to me.</td>
<td>5</td>
<td>9</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>A2.2.13 I believe my answer to the question above is the optimal state of things.</td>
<td>1</td>
<td>6</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.14 My work with privacy compliance makes use of automation tools.</td>
<td>1</td>
<td>9</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.15 I am familiar with the concept of Privacy-Enhancing Technologies (PETs).</td>
<td>8</td>
<td>11</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.16 PETs are among some of the best current methods for being compliant to privacy regulations (regarding the &quot;technical measures&quot;).</td>
<td>3</td>
<td>9</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.17 I feel like there is a lack of proper characterization of PETs (how they work, benefits, disadvantages, etc.)</td>
<td>2</td>
<td>12</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.18 PETs are actually quite difficult to implement in practice.</td>
<td>2</td>
<td>7</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>A2.2.19 The ability to implement PETs is very dependent on a company’s resources.</td>
<td>6</td>
<td>10</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.20 In general, the understanding of PETs requires a sound technical baseline.</td>
<td>4</td>
<td>11</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>A2.2.21 Communicating about these PETs with people with purely legal background is quite difficult.</td>
<td>3</td>
<td>6</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.22 There is no clear sense of how PETs relate to privacy regulations.</td>
<td>0</td>
<td>6</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>A2.2.23 I believe there is a general need for better education on PETs.</td>
<td>6</td>
<td>12</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>A2.2.24 I personally am interested in learning more about PETs.</td>
<td>7</td>
<td>10</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>A2.2.25 Specifically, I would like to learn more about PETs regarding: *</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>A2.2.26 There is a general lack of technical literacy when it comes to privacy compliance.</td>
<td>3</td>
<td>10</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>A2.2.27 There does not exist a solid technical framework for privacy compliance.</td>
<td>0</td>
<td>10</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.28 I believe there is little incentive to put resources into implementing the newest, state-of-the-art Privacy-Enhancing Technologies.</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>A2.2.29 It is more convenient and/or economical not to put time and resources into implementing sound technical measures.</td>
<td>0</td>
<td>10</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>A2.2.30 I believe that there are many technologies for data protection, yet the awareness and knowledge surrounding them is lacking.</td>
<td>2</td>
<td>15</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>A2.2.31 Privacy compliance doesn’t motivate the innovation of technology in the privacy field.</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>A2.2.32 I have an established point of contact in the case I have questions or concerns regarding privacy compliance.</td>
<td>5</td>
<td>9</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.33 I regularly interact with a Data Protection Officer or similar role.</td>
<td>8</td>
<td>5</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>A2.2.34 If the contact you regularly interact with is not a Data Protection Officer, please name the role: *</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>A2.2.35 When it comes to interpreting privacy regulations, this interpretation comes from the management level within my organization.</td>
<td>2</td>
<td>1</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>A2.2.36 I believe there are many ways to approach privacy compliance, specifically regarding technical measures.</td>
<td>7</td>
<td>13</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.37 There is an inequality in the current industry as to what suffices as &quot;being compliant&quot;.</td>
<td>5</td>
<td>11</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.38 The politics within an organization may affect the degree to which sound technical measures are pursued.</td>
<td>9</td>
<td>10</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.39 More focus should be placed on &quot;privacy engineering&quot; within organizations.</td>
<td>8</td>
<td>11</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.40 On the whole, I say legal support is readily available to me regarding any privacy-related matters.</td>
<td>5</td>
<td>14</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>A2.2.41 The implementation of technical measures for privacy compliance can be challenging depending on what systems are involved.</td>
<td>8</td>
<td>13</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>A2.2.42 Privacy compliance can be a bit of a &quot;gray area&quot;.</td>
<td>3</td>
<td>16</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.43 When it comes to technical measures for privacy compliance, the largely becomes a financial matter (creates a significant overhead).</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>A2.2.44 Demonstrating sound privacy compliance can actually boost a company’s value.</td>
<td>12</td>
<td>8</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.45 At the core of implementing technical measures for privacy compliance is a risk assessment, which is dependent on organizational culture.</td>
<td>5</td>
<td>13</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.46 I believe that the amount of privacy regulations nowadays makes implementing technical privacy measures considerably.</td>
<td>0</td>
<td>7</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>A2.2.47 There is a clear need for better &quot;harmonization&quot; of these regulations (and requirements).</td>
<td>3</td>
<td>17</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>A2.2.48 Privacy compliance involves too much bureaucracy.</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>A2.2.49 All in all, I think recent years have seen the industrialization of privacy (compliance).</td>
<td>6</td>
<td>11</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>A2.2.50 This industrialization is in my view a positive advancement.</td>
<td>5</td>
<td>11</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>A2.2.51 It is often the case with privacy compliance that although compliance can be argued for, true protection of privacy may not be achieved.</td>
<td>5</td>
<td>10</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.52 There is such a thing as &quot;over-compliance&quot;.</td>
<td>4</td>
<td>7</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>A2.2.53 In general, I think the concept of privacy itself is quite vague or not well-defined.</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>A2.2.54 The meaning of privacy is distinct from, and often conflated with, the concept of data protection.</td>
<td>4</td>
<td>8</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>A2.2.55 Being 100% compliant does not imply 100% data protection.</td>
<td>9</td>
<td>7</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>A2.2.56 The true meaning of privacy has been lost in modern privacy compliance.</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>6</td>
</tr>
</tbody>
</table>

Table B.2.: The Complete Survey Results, Tabular Format

**Total: 243**
Explanatory Notes

The complete survey results are presented in tabular format in Table B.2. For simplicity, “N/A” responses are not tallied. Totals for each response option are included at the bottom.

Questions with asterisks (and dashes in the counts) are questions of a different format than the rest. The results for these are included below in Figures B.1 and B.2.

Two particular questions originally included in the survey were omitted, namely A2.4.8 and A2.4.9 due to a clerical error.

A2.3.12

Specifically, I would like to learn more about PETs regarding (feel free to use the "other" option!)

23 responses

<table>
<thead>
<tr>
<th>Option</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Their advantages, disadvantages</td>
<td>13</td>
<td>56.5%</td>
</tr>
<tr>
<td>How they work (high-level)</td>
<td>10</td>
<td>43.5%</td>
</tr>
<tr>
<td>How they work (technically)</td>
<td>13</td>
<td>56.5%</td>
</tr>
<tr>
<td>N/A</td>
<td>5</td>
<td>21.7%</td>
</tr>
<tr>
<td>How to incorporate PETs in small to medium sized businesses</td>
<td>1</td>
<td>4.3%</td>
</tr>
</tbody>
</table>

Figure B.1.: A2.3.12

A2.4.3

Responses to the question included: IT Security, Lawyers, Privacy Specialists, Privacy Officer, Head of IT, Legal Counsel.
List of Figures

3.1. Time to adopt PETs! ................................................................. 13
5.1. Visualizing the Contact Process ..................................................... 24
5.2. Contacts, broken down by category .................................................. 25
5.3. Interviewee Years of Experience (in Privacy) ....................................... 26
5.4. Interviewee Accumulated Years of Experience ..................................... 27
5.5. Years of Experience, Pre- and Post GDPR Adoption ............................ 27
5.6. Interviewee Gender ........................................................................... 28
5.7. Interview Gender, broken down by sector ............................................ 29
5.8. Location of Interviewees and their Organizations .................................. 30
6.1. The Privacy Compliance Structure ..................................................... 46
7.1. Challenge Category 1 Mapping ......................................................... 60
7.2. Challenge Category 2 Mapping ......................................................... 76
7.3. Challenge Category 3 Mapping ......................................................... 91
7.4. Challenge Category 4 Mapping ......................................................... 107
8.1. Respondent Makeup, Roles ............................................................. 110
8.2. Respondent Makeup, Years of Experience ......................................... 111
8.3. Respondent Makeup, Organization Size ............................................ 112
8.4. Respondent Makeup, Technical or Legal .......................................... 113
8.5. A2.2.6 Results ................................................................................. 114
8.6. A2.2.9 Results ................................................................................. 115
8.7. A2.2.11 Results ................................................................................ 115
8.8. A2.2.3 Results ................................................................................ 116
8.9. A2.2.4 Results ................................................................................ 117
8.10. A2.2.12 Results .............................................................................. 117
8.11. A2.3.4 Results ................................................................................ 118
8.12. A2.3.7 Results ................................................................................ 118
8.13. A2.3.10 Results .............................................................................. 119
8.14. A2.3.17 Results .............................................................................. 119
8.15. A2.3.18 Results .............................................................................. 120
8.16. A2.3.14 Results .............................................................................. 120
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.17</td>
<td>A2.3.15 Results</td>
<td>121</td>
</tr>
<tr>
<td>8.18</td>
<td>A2.3.16 Results</td>
<td>121</td>
</tr>
<tr>
<td>8.19</td>
<td>A2.4.5 Results</td>
<td>122</td>
</tr>
<tr>
<td>8.20</td>
<td>A2.4.6 Results</td>
<td>122</td>
</tr>
<tr>
<td>8.21</td>
<td>A2.4.7 Results</td>
<td>123</td>
</tr>
<tr>
<td>8.22</td>
<td>A2.4.10 Results</td>
<td>123</td>
</tr>
<tr>
<td>8.23</td>
<td>A2.4.15 Results</td>
<td>124</td>
</tr>
<tr>
<td>8.24</td>
<td>A2.4.4 Results</td>
<td>124</td>
</tr>
<tr>
<td>8.25</td>
<td>A2.4.2 Results</td>
<td>125</td>
</tr>
<tr>
<td>8.26</td>
<td>A2.4.14 Results</td>
<td>125</td>
</tr>
<tr>
<td>8.27</td>
<td>A2.5.2 Results</td>
<td>126</td>
</tr>
<tr>
<td>8.28</td>
<td>A2.5.10 Results</td>
<td>126</td>
</tr>
<tr>
<td>8.29</td>
<td>A2.5.5 Results</td>
<td>127</td>
</tr>
<tr>
<td>8.30</td>
<td>A2.5.3 Results</td>
<td>127</td>
</tr>
<tr>
<td>8.31</td>
<td>A2.5.11 Results</td>
<td>128</td>
</tr>
<tr>
<td>9.1</td>
<td>Solution Concept - Challenge Mapping</td>
<td>143</td>
</tr>
<tr>
<td>9.2</td>
<td>Solution Concept Scores</td>
<td>146</td>
</tr>
<tr>
<td>10.1</td>
<td>Accumulated Interviews Over Time</td>
<td>150</td>
</tr>
<tr>
<td>10.2</td>
<td>otter.ai</td>
<td>151</td>
</tr>
<tr>
<td>10.3</td>
<td>MAXQDA Dictionary in Action</td>
<td>152</td>
</tr>
<tr>
<td>10.4</td>
<td>Call for Survey Participants</td>
<td>154</td>
</tr>
<tr>
<td>B.1</td>
<td>A2.3.12</td>
<td>173</td>
</tr>
</tbody>
</table>
List of Tables

5.1. Coded Interviewee Table ................................................. 31

7.2. Challenge Category 2, Technologies ..................................... 61
7.3. Challenge Category 3, Organizational Factors ............................ 77
7.4. Challenge Category 4, General ........................................... 92

8.1. Survey-Challenge Mapping .................................................. 109

9.1. Solution Concept Overview ................................................ 130

10.1. Qualitative Data Analysis Codified Table, Abridged .................... 153

B.1. The Complete Coded Challenge Table ................................... 170
B.2. The Complete Survey Results, Tabular Format .......................... 172
Acronyms

DPO  Data Protection Officer
GDPR  General Data Protection Regulation
IAPP  International Association of Privacy Professionals
PET  Privacy-Enhancing Technology
Bibliography


[27] International Association of Privacy Professionals. url: https://iapp.org/.


[38] Using thematic analysis in psychology. URL: https://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa.


[58] D. Huth and F. Matthes. ““Appropriate Technical and Organizational Measures”: Identifying Privacy Engineering Approaches to Meet GDPR Requirements”. In: (2019).


[79] URL: https://iapp.org/about/what-is-privacy/.


[88] URL: https://iapp.org/certify/.

[89] URL: https://privacypatterns.org/patterns/.


