

# Global Miscommunication in Privacy Requirements Engineering: Legal Experts' Experiences Collaborating with Software Engineers

Claudia Negri-Ribalta<sup>1</sup>  

ULIDE, University of Luxembourg, Luxembourg

Ioana Visescu  

ULIDE, University of Luxembourg, Luxembourg

Muriel-Larissa Frank  

FINATRAX, SnT, University of Luxembourg, Luxembourg

Anastasia Sergeeva  

IRiSC, SnT, University of Luxembourg, Luxembourg

Alberto García Simon  

Polytechnic University of Valencia, Spain

Rene Noel  

Escuela de Ingeniería Informática, Universidad de Valparaíso, Chile

Lorena Sánchez Chamorro  

Human-Media Interaction Research Group, University of Twente, The Netherlands

---

## Abstract

**Background.** Regulatory data protection requirements (RDPRs) impose requirements on organizations, which translate into technical and organizational measures for their information systems (IS). Meeting these requirements necessitates the collaboration between interdisciplinary teams of lawyers and software engineers. Previous studies indicate that engineers often struggle to interpret and translate RDPRs. Conversely, little is known about the experiences of lawyers when working on RDPRs in interdisciplinary teams, even though their legal interpretations shape the requirements imposed on IS.

**Aim.** Therefore, this paper seeks to unpack the challenges that lawyers face when collaborating with software engineers to implement data protection requirements and to put them in motion in case of privacy breaches.

**Method.** Through a deductive qualitative analysis, this paper analyzes semi-structured interviews with 70 data protection lawyers from 25 countries. Results: Our findings highlight that lawyers throughout regions and regardless of their cultural background describe similar challenges when collaborating with engineers: a lack of shared language and mental models. Lawyers also point out that engineers misunderstand RDPRs for various reasons, not just a lack of education. Furthermore, we identify the key elements that hinder or facilitate collaboration and their implications for privacy engineering.

**Conclusions.** This study is a large qualitative research with participants from multiple countries. Our results suggest that lawyers perceive different challenges when collaborating with software engineers, regardless of their culture. These results suggest these challenges are structural rather than cultural. Organizations should prioritize developing methods and artifacts to overcome these challenges.

**2012 ACM Subject Classification** Security and privacy → Social aspects of security and privacy; Software and its engineering → Requirements analysis; Human-centered computing → User studies

---

<sup>1</sup> Corresponding author



© Claudia Negri-Ribalta, Ioana Visescu, Muriel-Larissa Frank, Anastasia Sergeeva, Alberto García Simon, Rene Noel, and Lorena Sánchez Chamorro;  
licensed under Creative Commons License CC-BY 4.0

20th International Symposium on Empirical Software Engineering and Measurement (ESEM 2026).  
Editors: Robert Feldt, Maria Paasivaara, Daniel Mendez, Stefan Wagner, and Marvin Muñoz Barón;  
Article No. 14; pp. 14:1–14:22



Leibniz International Proceedings in Informatics  
LIPIC Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

**Keywords and phrases** data protection, mental models, privacy, collaboration

**Digital Object Identifier** 10.4230/LIPIcs.ESEM.2026.14

**Category** Technical Track Paper

#### Supplementary Material

*Dataset (Zenodo repository):* <https://doi.org/10.5281/zenodo.15166882>

**Funding** *Claudia Negri-Ribalta:* This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Actions grant agreement 101081455

*Muriel-Larissa Frank:* This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant ref. 13342933/Gilbert Fridgen.

*Lorena Sánchez Chamorro:* This work has been conducted under the realm of the RESOCIAL project, funded by the Dutch Research Council NWO under the Synergy Theme: Vulnerability and resilience in an online society (grant number NWA.1540.21.001)

**Acknowledgements** The authors would like to thank Dr. Marius Lombard-Platet for his support.

## 1 Introduction

Regulatory data protection requirements (RDPR) need interdisciplinary teams to satisfy them [25] as they shape the design of information systems (IS). For instance, a data subject exercising their right of access is a RDPR that demands a process that teams must anticipate when designing the system. This means that it is necessary from the very start to know what data is held, where, for how long, to be able to verify a request’s lawfulness and fulfill it on demand.

Thus, legal or technical expertise alone does not suffice for satisfying and specifying RDPRs, as their analysis demands multiple types of knowledge. Across the different stages of the requirements engineering (RE) lifecycle, both legal and technical expertise are required: lawyers<sup>2</sup> establish the interpretative foundations of regulatory obligations, while software engineers translate these requirements and specifications, as neither discipline can effectively address these challenges in isolation, but rather in an interdisciplinary collaboration. Previous work highlights the necessity of interdisciplinarity for RDPRs and its challenges [37, 28, 46]. Interdisciplinarity and working in cross-functional teams can be difficult, as legal requirements are typically formulated in abstract and context-dependent terms, which clash with the expectations coming from requirements engineering that specifications should be precise, unambiguous, and measurable [10, 31].

Even when legal experts are involved, translating such open-textured norms into IS requirements and specifications remains challenging, as it requires interpreting broad legal concepts into measurable requirements [9], while achieving a shared understanding between domains [46, 19]. This gap can create friction, which may result in poorly elicited requirements, misunderstandings, and ultimately costly rework or non-compliant software [31]. The longer a poorly understood and inadequately analyzed requirement persists, the more expensive it becomes to modify, with a considerable number of projects failing as a result [31, 10, 46].

It is essential that RDPRs are correctly understood by these interdisciplinary teams from the early phases of the software development lifecycle (SDLC). Multiple studies suggest that software engineers struggle to translate RDPRs, due to legal complexity [25], different mental

---

<sup>2</sup> In this paper, the word lawyer defines any legal expert, barred or not, with knowledge on the topic of data protection. The term lawyer is used interchangeably with legal expert.

models [23], or difficulties comprehending its legal implications [24], among others. Furthermore, the lack of a shared understanding [19] directly impacts the software development, particularly across cross-functional teams [46]. In the context of data protection, poorly analyzed and understood RDPRs can lead to privacy breaches [46]. Hence, having a shared understanding of requirements among interdisciplinary and cross-functional teams is vital for organizations to adopt good requirements engineering (RE) practices and well-developed information systems (IS) [10, 46].

Given the role lawyers play in the SDLC for RDPRs, it is important to understand their perceptions and requirements regarding this topic. This article stands at the intersection of human factors and RE, recognizing that lawyers play a central role in shaping the conceptualization of RDPRs. If lawyers cannot express the correct conceptualization of a requirement, it will have consequences for system development, ranging from expensive rework to non-compliance.

**Our goal is to understand how lawyers worldwide experience collaboration with software engineers in data protection requirements. We therefore divide our analysis in the following subquestions.**

- **RQ1: What challenges do lawyers identify when collaborating in interdisciplinary teams for data protection?**
- **RQ2: What factors do lawyers believe contribute to the difficulties software engineers have in interpreting and implementing data-protection regulations?**
- **RQ3: How do lawyers understand and fulfill their roles within interdisciplinary teams in the event of a personal data breach?**

To address the research question, we conducted a qualitative study using semi-structured interviews with 70 data protection lawyers from 25 countries worldwide. Using a qualitative deductive analysis (QDA) approach, we reveal *that lawyers in different countries experience the same challenges and face similar perceptions of interdisciplinary collaboration, regardless of their culture*. Most participants highlight that the lack of a common language and unshared conceptualization of RDPRs negatively impact their work, even across different jurisdictions. They acknowledge that legal requirements are difficult for software engineers to understand. At the same time, lawyers are frustrated as they spend more time explaining to engineers how to satisfy RDPRs. This time could have been used for other activities if there had been a shared understanding. Generally, software engineers could resort to artifacts<sup>3</sup> to establish common ground. However, lawyers seem to lack knowledge over these tools, thus the common ground is harder to establish.

**These results lead us to conclude that lawyers are, at best, unaware of communication artifacts developed by the RE community and, at worst, these artifacts fail to meet their expectations. It also suggests that, regardless of a country's data protection culture, lawyers' experiences collaborating with computer scientist/software engineers are similar: they lack shared understanding, that goes beyond a common language but a shared conceptualization.** Furthermore, the results show the need to promote empathy when collaborating within interdisciplinary teams in data protection.

The remainder of the paper is organized as follows: Section 2 provides related work on the subject. Section 3 describes the research method used while Section 4 presents the results, which are organized by research question and key findings. Section 5 discusses practical implications and future work. Section 6 addresses the limitations, and Section 7 our conclusions.

---

<sup>3</sup> We frame artifacts following [48].

## 2 Related work

### 2.1 Data protection and privacy requirements

Organizations must adhere to various regulations, including those related to privacy and data protection. From a conceptual standpoint, privacy and data protection requirements are not the same [17]. Privacy can have multiple meanings [39, 17], and may overlap with data protection when processing personal data is linked to a person's privacy [17]. Hence, data protection is the materialization of privacy for the management of personal data [17]. In other words, data protection deals with managing personal data due to the difficulty of encompassing all privacy requirements and stakeholder expectations [47].

Prior work has shown that vague privacy requirements can lead organizations to produce incomplete responses that do not sufficiently address core privacy threats in system design [20]. Translating these regulatory requirements, including those pertaining to data protection, into software requirements presents a significant challenge [8, 23, 46, 4, 35]. As a result, multiple artifacts have been proposed to manage the work with data protection requirements worldwide [13, 28, 18]. [1] use to propose different patterns for analyzing consent, data breaches, and subjects' rights under the GDPR. Similarly, the Unified Modeling Language (UML) has been considered as a possible means of addressing GDPR requirements, though further research is needed to confirm the suitability of such an approach [44]. From a goal-oriented requirements engineering perspective, both [34] and [29] used the Socio-Technical Security modeling language (STS-ml) for specific aspects of the regulation. [2] proposed the "Guide me" framework, which consists of a six-step systematic approach to eliciting and connecting GDPR requirements to privacy obligations. [28] provide a mapping study of regulatory data protection. The novelty of our work lies in researching lawyers' challenges when working with privacy requirements with software engineers from a global perspective, rather than focusing on software engineers' challenges, as most previous literature does.

### 2.2 Organizational challenges for data protection requirements

Although software engineers acknowledge the importance of privacy practices, they rarely implement such mechanisms in their software designs [30, 8]. Previous studies have attempted to explain this discrepancy by identifying various organizational barriers, such as organizational culture [33], or individual barriers, such as a lack of knowledge [35] for this phenomena.

Many software engineers do not view privacy as a functional requirement and believe that privacy requirements are ineffective or satisfied with security measures [36, 23], and conflicting with other software requirements [4, 35]. This perception is exacerbated by the fact that privacy and data protection requirements are considered as "vague" [39, 4] and difficult to satisfy [23, 4, 35]. Consequently, it is difficult for engineers to translate privacy requirements into practice or to prioritize them [30]. This becomes even more difficult when engineers work across multiple jurisdictions [32]. Matters are further complicated by the fact that many engineers lack formal education in privacy theories [35, 30]. Instead they are self-taught and struggle with legal terminology [32]. This is due to the fact that legal texts are written in a specific domain manner which makes their translation complex and demands knowledge of other legal instruments [9]. As a result, engineers use security vocabulary as synonymous with of privacy, even though the two are not the same and serve different purposes [23]. Additionally, implementing privacy requirements becomes burdensome [4], and engineers deliberately choose not to prioritize them over functional system requirements [35].

Additionally, engineers have difficulty mapping privacy principles into software features because of their complexity [35]. In other cases, they overlook the regulatory context [37] or do not feel responsible [40, 45]. Another issue is interdisciplinary collaboration, as engineers experience frustration with legal teams [4] or have difficulties having a shared around non-functional requirements [46]. Furthermore, software engineers recognize that collaborating with lawyers and cross-functional teams is challenging [4, 8].

In terms of organizational challenges, lack of agency [40] and time pressure are key factors impeding implementation of privacy requirements as engineers do not enjoy working in such an environment. Even when trying to promote privacy through “privacy champions”, these roles encounter strong resistance due to a negative culture towards privacy, tensions among stakeholders, or lack of support [43]. These experiences with privacy-driven engineering roles can reveal the need to understand other stakeholders’ needs to support engineers in implementing privacy requirements. Our work contributes to this need by identifying, on a global scale, the challenges lawyers face when providing privacy expertise to software engineers.

### **3 Research Method - qualitative deductive analysis (QDA)**

The Qualitative Data Analysis (QDA) method is a deductive approach designed to test, refine, or reformulate theory [15], while also incorporating elements of inductive analysis. The method consists of the five following key steps. The leading author also kept a memoing of the whole process [5].

1. Defining the research questions and theoretical framework [15]. Researchers position their study within a theoretical or conceptual framework informed by prior work, consistent with a deductive orientation. In this study, our research question examines how lawyers worldwide collaborate with software engineers on data protection requirements. For our theoretical background, we follow the guidance of [5] and build upon [23, 42, 19] from a requirements engineering perspective. Specifically, we focus on the concepts of common ground, implicit shared understanding, and data protection, drawing on the Data Protection Brussels Effect [6], with particular emphasis on the role of the GDPR in requirements engineering [28].
2. Operationalizing Theory: Core constructs, codes, or hypotheses are developed based on existing literature [5] and may be refined during preliminary analysis. Inductive codes can be incorporated where necessary. While developing our code, we could not find a codebook from prior work that aligns with our research objective. As such, we built the codebook to answer our question and, based on previous literature, as suggested by [5], for a deductive analysis. From RE, we based our codes on [23, 42, 19] and for the Brussels Effect, based on the GDPR [14, 28, 6]. Our codebook also allowed for inductive codes (which we indicate in this paper). The codebook was developed through multiple iterations, as we explain in detail in Section 3.3, as part of the sensitizing phase of QDA [15].
3. Sampling: Purposive sampling [3, 15] is employed, including the intentional selection of negative or contradictory cases to challenge or extend the guiding framework. Specifically, we recruited participants from selected countries (G20 plus invitees) with expertise in data protection law. Further details on the sampling process are provided in Section 3.2.
4. Coding and Analyzing: Data is systematically coded and examined in relation to the predefined constructs and emerging themes. An early round of analysis was conducted to further sensitize the codes [15] and to identify any overlooked areas. Coding and

intermediate analysis [15] were performed by five authors, with each interview coded by at least two authors. The coding and analysis procedures are described in detail in Section 3.3.

5. Theorizing: Findings are interpreted to test, elaborate, or, where needed, reformulate the underlying theoretical framework. This part implies “theorizing, which involves interpreting evidence for each of the themes, proposing interconnections between them, and providing a rationale for any revisions or expansions to the initial theory” [15].

### 3.1 Operationalizing Theory

To develop the codebook, we followed the guidance provided by [5]. Since our codes were constructed for a deductive analysis [15], and no codebook from previous work seemed suited, we elaborated the codebook based on established theory and anticipated outcomes. Our codebook drew on both the Brussels Effect for data protection regulation (GDPR) [6, 14, 28] and prior research on data protection, privacy requirements, and shared understanding [23, 19, 42]. We developed the codebook iteratively using the QDA method. The lead author drafted an initial version, which was subsequently reviewed and revised in collaboration with the co-authors. Following these revisions, the lead author validated the codebook with five lawyers from diverse jurisdictions (EU, Chile, Brazil, and China) to minimize potential bias. Their feedback was documented and integrated into the codebook. The revised codebook was then further discussed among the authors. During an early analysis, as recommended by [15] to sensitize the code, we identified areas that were initially overlooked. We added new indicative codes to address these gaps, as suggested by [15], thereby reducing potential bias and ensuring comprehensive data coverage.

### 3.2 Sampling - Participants and Recruitment

We conducted interviews with legal experts in data protection (N=70) from the G20 countries (including the European Union and the African Union as entities), due to the economical influence and population size. We also randomly selected invited countries to the G20 summits (Chile, Colombia, Egypt, Tanzania, Azerbaijan, Indonesia and Singapore) and Luxembourg (country where the study was carried). We excluded practitioners from Russia due to sanctions in place at the time of ethical approval. We explain the recruitment process below, but overall we recruited experts based on their experience, education, known qualifications and peers recognition.

In our final sample of 70 interviews, there are no practitioners from Saudi Arabia and Azerbaijan, as they did not answer the request for interviews. Some of the participants have expertise from more than one jurisdiction, such as Brazil and EU, France and Germany or USA and EU. An anonymized overview of participants is available in the Table 1, based on the continent of expertise rather than country of expertise, for anonymization purposes. **We do not indicate the country (and years) of expertise, as many individuals have a unique profile that can easily re-identify them.** Some countries have a very small universe of data protection experts (such as Chile or Colombia), so any extra data point – such as area of work or years of study – could lead to the participant re-identification, which breaches their consent preferences. A more detailed but still anonymous list of our participants is available in our public repository, made available at out at Section 8. Finally, some of our participants are public figures, like data protection authorities or ex-ministers, so the sensitivity of their interviews increases the need of anonymization.

■ **Table 1** Summary of the participants expertise, based on continent of residence. Junior = 2–3 years experience; Intermediate = 4–8 years experience; Expert = +8 years experience.

| Num. of<br>Participants | Region |                  |        |               |               |
|-------------------------|--------|------------------|--------|---------------|---------------|
|                         | Africa | Asia and Oceania | Europe | North America | South America |
| Expert                  | 7      | 13               | 15     | 9             | 12            |
| Intermediate            | 3      | 7                | 0      | 0             | 3             |
| Junior                  | 0      | 1                | 0      | 0             | 0             |

The initial goal was to interview at least 3 experts per country, with a maximum of 5. This precondition was not achieved for Australia and Germany, with 2 and 1 participant respectively, although more than 15 invitations per country were sent out. For the participants who had multiple jurisdiction expertise, their participation would satisfy the requirement of multiple countries.

We searched for participants based on their public profiles. We queried multiple legal databases of private organization, academic publishing, public authorities, and social media (LinkedIn). Participants were first contacted either by email (if public) or their professional network (LinkedIn). We resorted to snowballing in the countries where we had difficulties contacting individuals otherwise, with 8 participants recruited this way. In total, 267 invitations to practitioners from all over the world were sent between December 2024 and November 2025. Table 1 provides an overview of the participants. Due to space constraints, we provide further details of the recruitment process in the public repository available at Section 8.

All interviews were conducted with participant informed consent. Where permission to record was granted, interviews were audio-recorded and transcribed, otherwise detailed notes were taken to capture key phrases and central points. Interviews lasted 35 minutes on average. To establish rapport and ensure participant comfort, the first part of the interview was dedicated to an informal discussion of the study. This segment was not recorded and is excluded from the study.

Interviews were conducted in English, Spanish, or French. The majority were carried out online via the platform provided by the research institution (Microsoft Teams), while eight interviews were conducted in person. When recording consent was obtained, audio files were transcribed using AIKO, an open-source, locally deployed, privacy-preserving AI-based transcription tool. During transcription and editing, minor filler words and unnecessary repetitions were removed to enhance readability, while intentionally retaining selected speech particularities to preserve the integrity and texture of participant expressions. In presenting the quotes, ‘[ ]’ was added where sensitive details were removed due to anonymization.

The interviews are part of the OBI-PIA project, that seeks to identify RDPRs across jurisdictions. The interview questions are available at our public repository.

3.3 Coding and Data analysis

For the coding and analysis of the interviews, three calibration workshops were held between coders throughout 2025, two of which were recorded. During these, the authors discussed how they had coded the same interview and shared their results, with a discussion if discrepancies occurred. The objective was to have calibration between the different coders, while also solving any question regarding the conceptualization of the codes.

Five authors partook on the coding of the interviews. Each interview was coded by at least two authors. One author would carry out the first coding, send the file(s) to the second coder, who would code on top of the first coder, and see if they identify discrepancies. If

■ **Table 2** Example on how codes and subcodes were coded.

| Theme                         | Code                           | Subcode             | Example of coding                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|--------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interdisciplinarity (theme)   | Lack of common language (code) |                     | <i>"We don't speak the same language. I mean, although it's the same language, because we do it in English, or even if it's in French, when it's our mother tongues... I have the impression we don't speak the same language".</i>                                                                                                |
|                               |                                |                     | <i>"Sometimes to make the bridge, the connection between the two, which are nothing that we cannot overcome, but yeah, just to be mindful".</i>                                                                                                                                                                                    |
|                               | Communication (code)           | Difficult (subcode) | <i>"Originally the communication was very difficult with the technical teams".</i>                                                                                                                                                                                                                                                 |
| Understanding data protection | Lack of education              |                     | <i>"They lack the literacy and also there is a lack of guidance for them to understand it and do that, and sometimes you have to push them".</i>                                                                                                                                                                                   |
|                               |                                | Per lawyers in tech | <i>"The lawyer actually must have a very open mind to understand technology as well and this is that's the I think that's the difficult aspect because most engineers could at some point understand law but it doesn't go the other way around because I mean lawyers it's very hard to explain technical things to lawyers".</i> |

discrepancies happened, they were resolved through consensus. Finally, if no consensus was reached, the lead author would arbitrate. This method allows us to reduce biases in our the analysis, while also improving the reliability of it. The coding was done using MaxQDA. An example of how we coded the different excerpts of data, Table 2 provides an example overview. Given space limitations, a full detailed description of the codebook is available at our public repository.

### 3.4 Ethical considerations

This research aims to follow best practices in qualitative studies and ethical software engineering interviews [41]. Participants in the study were presented with the project's privacy policy and information notice. They also received a consent form. The form was granular, allowing participants to opt in to each option: processing personal data, recording, using AI transcription tools, sharing transcripts, and possible recontact. Participants would sign the consent form. If the participants forgot to send the consent forms before the agreed-upon interview meeting, an oral consent was requested before the interview started, which also included whether we could record. Every other option in the consent form was considered a non-opt-in. Except for 5 individuals, all others consented to have their interviews recorded. 3 other participants requested to send written answers for the same reason.

Participants did not receive monetary compensation and were informed beforehand in the invitation email. However, they will be granted access to the study results. This research received approval from the Ethical Committee under code ERP 24-109 OBI-PIA from the University of Luxembourg. We provide a positionality statement as part of the Section 6 and an extended version at the public repository.

## 4 Results and findings

Given the study design, not all participants answered every question due to time constraints or choice. Tables 3 and 4 (Pages 9 and 14, respectively) are therefore reported as the number of participants addressing each topic. For example, the code "Data Breaches" was mentioned at least once by 58 participants, while the code "incident" appeared in 43 accounts, including discussions of "incident response", "containment", or "internal notification". A participant addressing multiple subtopics is counted once at the code level ("incident Responses") but may be recorded across several subcodes ("containment", "internal notification"); conversely,

■ **Table 3** Table for codes regarding interdisciplinary challenges for data protection and understanding of data protection. Codes are unique instances, subcodes can overlap between participants. †: Inductive codes.

| Theme                         | Code | Subcode                   | Number of occurrences (percentage of n in column) |                  |                     |                  |                      | Total<br>n = 70   |
|-------------------------------|------|---------------------------|---------------------------------------------------|------------------|---------------------|------------------|----------------------|-------------------|
|                               |      |                           | Asia, Oceania<br>n = 21                           | Africa<br>n = 10 | N. America<br>n = 9 | Europe<br>n = 15 | S. America<br>n = 15 |                   |
| Interdisciplinarity           |      |                           | 18 (85.7%)                                        | 9 (100.0%)       | 9 (100.0%)          | 15 (100.0%)      | 15 (100.0%)          | <b>67 (95.7%)</b> |
|                               | —    | Lack of common language   | 11 (52.4%)                                        | 5 (50.0%)        | 8 (88.9%)           | 12 (80.0%)       | 10 (66.7%)           | <b>46 (65.7%)</b> |
|                               | —    | Different mental models   | 13 (61.9%)                                        | 3 (30.0%)        | 6 (66.7%)           | 10 (66.7%)       | 13 (86.7%)           | <b>45 (64.3%)</b> |
|                               | —    | Communication             | 4 (19.1%)                                         | 3 (30.0%)        | 2 (22.2%)           | 3 (21.4%)        | 4 (26.7%)            | <b>17 (24.3%)</b> |
|                               | —    | — Difficult               | 4 (19.1%)                                         | 2 (20.0%)        | 1 (11.1%)           | 1 (6.7%)         | 3 (20%)              | <b>11 (15.7%)</b> |
| Understanding data protection | —    | Lack of tech education†   | 1 (4.8%)                                          | 2 (20.0%)        | 1 (11.1%)           | 2 (13.3%)        | 2 (13.3%)            | <b>8 (11.4%)</b>  |
|                               |      |                           | 19 (90.0%)                                        | 10 (100.0%)      | 9 (100.0%)          | 15 (100.0%)      | 15 (100.0%)          | <b>68 (97.1%)</b> |
|                               | —    | Legalese (legal prose)    | 9 (42.9%)                                         | 6 (60.0%)        | 7 (77.8%)           | 6 (40.0%)        | 7 (46.7%)            | <b>35 (50.5%)</b> |
|                               | —    | Lack of education         | 11 (52.4%)                                        | 6 (60.0%)        | 4 (44.4%)           | 7 (46.7%)        | 6 (40.0%)            | <b>34 (48.6%)</b> |
|                               | —    | — Lawyers in tech         | 2 (9.5%)                                          | 2 (20.0%)        | 1 (11.1%)           | 2 (13.3%)        | 2 (13.3%)            | <b>9 (12.7%)</b>  |
|                               | —    | Mental model perceptions† | 8 (38.1%)                                         | 5 (50.0%)        | 6 (66.7%)           | 7 (46.7%)        | 6 (40.0%)            | <b>32 (45.7%)</b> |
|                               | —    | Explicit agreement†       | 6 (28.6%)                                         | 2 (20.0%)        | 4 (44.4%)           | 2 (14.3%)        | 8 (53.3%)            | <b>22 (33.9%)</b> |
|                               | —    | Incentive issues†         | 1 (4.8%)                                          | 2 (20.0%)        | 1 (11.1%)           | 4 (26.7%)        | 0 (00.0%)            | <b>8 (11.4%)</b>  |
|                               | —    | Explicit disagreement†    | 0 (0.0%)                                          | 0 (00.0%)        | 1 (11.1%)           | 1 (11.1%)        | 4 (26.7%)            | <b>6 (8.6%)</b>   |
|                               | —    | Resistance†               | 1 (4.8%)                                          | 0 (00.0%)        | 1 (11.1%)           | 3 (20.0%)        | 1 (6.7%)             | <b>6 (8.6%)</b>   |
|                               |      |                           | 1 (4.8%)                                          | 0 (00.0%)        | 1 (11.1%)           | 3 (20.0%)        | 1 (6.7%)             | <b>6 (8.6%)</b>   |

discussing a single subcode (“containment”) is counted both at the subcode level and within its parent code family. Verbatims from Spanish have been translated by the authors and the original ones are available at our public. All interview question are also available in the repository.

#### 4.1 RQ1: What challenges do lawyers identify when collaborating in interdisciplinary teams for data protection?

The majority of respondents (n=67, or 90.6%) shared they experienced challenges when working in interdisciplinary teams, as shown in Table 3. First, 46 participants mentioned language barriers (code “lack of common language”), meaning they lack the same vocabulary when discussing data protection requirements. Second, 45 participants highlighted having different mental models (code “different mental models”) about the topic. Furthermore, more than 20% of the respondents (n=17) expressed some kind of concern about communication in these teams, with 11 participants directly indicating that it was difficult. Finally, 8 participants stated that, in their view, the lack of technical education among lawyers made the interdisciplinarity between law and other disciplines difficult in the context of data protection.

Finding 1: Lawyers require an artifact to establish a common language or conceptualization with computer scientists or software engineers in regulatory data protection. This language needs to represent both stakeholders’ conceptualizations and goals, and should be easy to select.

##### 4.1.1 Lack of common language (46 participants)

Our analysis reveals that the vast majority of participants report issues due to the lack of a common language. As one participant explains: “[...] there’s constantly this challenge of translating different languages and finding common ground” (P.64). The main challenge for lawyers seems to be explaining what is needed from a regulatory perspective, in a way that is not simple a yes or no answer, as exemplified by the following: “I’ve been working for some years with several different teams on computer science, on the topics of data protection, and with different teams, in different [countries and organizations], the main issues were mostly about language” (P.33).

As participants explained, the role as a lawyer is not only to ensure compliance but also to reduce organizational risks. One participant explains: *“A lawyer’s objective is risk minimization always. What is the worst-case scenario? How can we minimize this? While engineers are sometimes looking from things from an innovative perspective. How can I circumvent rules? How can I find this issue and solve it? Which is very different from a lawyer’s way of thinking”* (P.3). It appears that lawyers bring a risk-oriented and context-sensitive mental model. While their technical counterparts may seek immediate and concrete implementation strategies, lawyers tend to focus on regulatory exposure, interpretive nuances, and long-term organizational impact.

Moreover, it seems legal experts seem to have difficulty explaining basic data protection concepts to software engineers: *“Maybe sometimes you say the same words, the same concepts, but they have a different content”* (P.10). As the quotes above indicate, problems arise because stakeholders from different disciplines often fail to clearly communicate or understand one another. For example, legal and technical staff may use the same word with different meanings, which can easily lead to misunderstandings, as one respondent notes: *“Different disciplines use almost the same terminology, but the usage of that terminology means completely different things. So I found that often conversations happen in parallel, that you may think you talk about the same thing, but when it boils down to technicalities”* (P.5). This lack of shared understanding results in spending more time than desired explaining what was meant or expected when discussing RDPRs: *“I think for most people, it’s just the basic concepts of data protection.”* (P.8).

However not everyone identifies the lack of common language as an issue. One participant reports: *“I don’t see it as much as a challenge as it is the first step in the relationship to clarify and manage expectations of what they mean or what we mean by certain things[...]"* (P.15). Some lawyers have even started using intermediate artifacts to establish common ground and a common language, albeit with difficulties: *“Of course, determining the right vocabulary for the right audience is something which is quite challenging”* (P.38).

#### 4.1.2 Different mental models (45 participants)

45 participants acknowledge that differing mental models hinder their collaborative work. As discussed in Section 2, software engineers often struggle to determine the precise requirements to satisfy RDPRs [7], and their mental models may contribute to this challenge [23]. As one participant observed: *“They will also say some words, maybe they have a common sense but you know the details and the actual definitions are different”* (P.12). Although the same term may be used, lawyers and engineers often attach different conceptualizations to it. These nuanced differences in the details are where the different mental models come into play: *“The concept of privacy for computer scientists, at least in my experience, was mostly referring to protection from identification, while in the law, privacy is a whole bunch of topics, all coming from the protection of private and family life”* (P.40).

Even when using the same vocabulary, lawyers and engineers differ in the degree of determinacy they expect and their tolerance for ambiguity. They also differ in their approach to RDPRs: lawyers primarily view them as normative risk assessments, while engineers primarily view them as operational design constraints. One of our participants lays out this distinction: *“People with a humanities background are quite comfortable with a certain level of ambiguity or uncertainty, while people with a technical background feel very uncomfortable and prefer to have straightforward answers, so I don’t think it’s really a matter of having difficulty understanding the concepts...”* (P.33). This different approach was shared by different

participants, like: “[...] the engineers in our team want to come up with a mathematical formula, while the lawyers want to come up with these complex concepts and fundamental rights” (P.64).

#### 4.1.3 Communication (17 participants)

Some of the participants ( $n = 17$ ) identified communication itself as a direct challenge, going beyond lack of common language or different mental models. The primary challenge is translating the abstract nature of RDPRs by lawyers into requirements specifications. As one participant stated: “... you have to deal with them and to try to be very clear and stay careful when they want to collect data” (P.42). Legal experts reported that engineers are often unable to correctly translate requirements into specifications, even when requirements are communicated and best practices from RE are applied: “They are unable to materialize it or translate this idea into a concrete action within their domain of practice” (P.56). This suggests a difficulty to move beyond disciplinary communication barriers.

2 participants acknowledged that this issue can be resolved, as long as both parties are willing to understand each other and make their best efforts. This situation is evidence of the importance of empathy and communication in RE [11, 46, 26]. Indeed, they shared that they have used UML to try to communicate RDPRs, recognizing it is not the best strategy. These references to intermediate artifacts were rare and were not systematically shared with participants. Thus, despite the substantial effort within the RE community to support interdisciplinary communication, existing artifacts have not permeated or resolved the practical realities of interdisciplinary RDPRs work, or at least not in the legal domain. These reflections suggest that interdisciplinary challenges are not only technical, but also relational. Effective collaboration appears to require an active effort to understand other stakeholders, as suggested by [46].

#### 4.1.4 Lack of technical education. (8 participants)

Another factor contributing to interdisciplinary challenges is the limited technical knowledge of some legal professionals. 8 participants (15.7%) explicitly referred to this issue. As one participant stated: “I mean, that goes in both ways as well, like trying to understand the limitations of technical systems” (P.52). Thus, collaboration challenges stem not solely from engineers’ limited legal knowledge, as discussed by the RE community [7], but also from lawyers’ limited understanding of technical constraints should be factored in. In fact, two participants emphasized that acquiring basic technical literacy improved communication with software engineers. One participant noted, “So now I’m actually understanding them and I can express myself to them” (P.32). This suggests that technical knowledge functions as a boundary-bridging competence within interdisciplinary teams.

### 4.2 RQ2: What factors do lawyers believe contribute to the difficulties software engineers have in interpreting and implementing data-protection regulations?

68 participants shared thoughts regarding this element throughout the interview, as shown in Table 3. When directly being prompted over the topic in question 3 of the interview, 22 participants (33.9%) explicitly said they agreed with the statement we prompted in question 3 of the interview, 2 that partially agreed, and 6 that they do not agree.

Finding 2: Most participants agreed that software engineers have difficulty understanding data protection for multiple reasons. Most lawyers agree that the way RDPRs are written makes it difficult to translate and understand. They also point out the role of education for understanding RDPRs. Furthermore, a minority of lawyers identified other reasons, such as poorly placed incentives and resistance from software engineers to learning about RDPRs. Finally, a minority of participants did not agree that software engineers had difficulty understanding RDPRs or that the issue had other reasons.

#### 4.2.1 Legalese (35 participants)

Most lawyers identified legal jargon as the main source of difficulty for translating RDPRs: *“often law is written in a weird manner”* (P.44); in other words, legalese. This difficulty arises due to multiple reasons, including the law’s ambiguity, the (multiple) interpretations of legal texts, the context and complexity of data protection regulations as recognized by previous RE research [28]. Participants emphasize that laws are often ambiguous and primarily written by and for lawyers. They are generally costly to create and update, so they are written in a way that allows them to be applied to many different situations. This ambiguity contradicts the specificity and well-defined requirements, leaving software engineers to interpret them. One respondent explains this: *“The law seems very vague. It’s very unclear. It seems very hard to implement. It seems to give no clear guidance”*(P.11). Similarly, another participant adds: *“[...] The regulation doesn’t tell them [software engineers] what they must do to achieve compliance”* P.25).

Given the possible multiple interpretations of legal texts, lawyers seek to determine the interpretation that best fits the context, yet they are reluctant to provide a definitive answer. They want to problematize the context and believe software engineers have difficulties understanding this approach: *“The relative or the absolute perspective. So they want yes, no, but we need to problematize it to put the landscape at stake, and they want yes and no answers. And for us, it’s more like it depends [...] And they do not deal well with open concept, open textured concepts”* (P.33).

Lawyers say it is important to review court decisions and interpretations to better translate RDPRs into requirements. Although the influence of case law differs between jurisdictions, this was important in all the regions we studied. As one participant said: *“And then you need to look at the case law, the decisions of courts, to understand what the interpretation of those terms”* (P.45).

#### 4.2.2 Lack of education (34 participants)

Navigating RDPRs requires understanding of legal concepts and nearly half of the respondents (n=34) reported that many software engineers lack this. One participant illustrates: *“Reading one law doesn’t make you a legal expert even in that law because lawyers or law students study many laws [...] they don’t have enough legal background”* (P.4) Without this foundation, software engineers risk mis-translating the requirements into incorrect specifications. One participant exemplifies, *“We have predefined requirement of consent. Sometimes people in technical roles don’t know how to interpret that”* (P.18). Legal education also helps with prioritization of RDPRs, which software engineers miscomprehend: *“But they don’t have this notion that you need to go beyond the text of a particular instrument to make sense of the legal system as a whole. And even when they can make sense of the pieces, they are waving different value sets. And it might not be obvious for them why [...]”* (P.65). As [46] also identified, the lack of shared understanding hurts the prioritization of privacy requirements.

However, technical education also helps the RE process. Therefore, lawyers themselves aspire to improve their knowledge, as the following statements indicates: *“The solution is for lawyers to understand a bit more about the technical processes. You don’t need to learn how to code, but you need to understand what coding is”* (P.3).

On the other hand, lawyers recognize their lack of technical education complicates matters for software engineers who must understand data protection requirements, as reported in subcode “Per lawyers in tech” (n=9). For example, one participant states: *“Well-intentioned regulatory or policy initiatives, end up disrupting how the internet functions, due to a lack of understanding of how things work”* (P.57, translated from Spanish).

#### 4.2.3 Incentives, disagreement, and resistance (resp. 8, 6, 6 participants)

Our analysis also revealed codes that had not been accounted for previously. These codes pertained to incentives (n=8), disagreement (n=6) and resistance (n=6). 8 participants agree that there are few incentives for companies or software engineers to incorporate RDPRs. As one participant states that there is a *“lack of incentivization for them to even learn it and apply it”* (P.13). Another participant argues that business models discourage compliance: *“Lot of organizations lack that incentive right because their business models and the way that they want to do things are all about kind of like monetizing of data”* (P.45). Additional explanations include domain-specific factors, as noted by participant 41 (medical domain versus data protection), or the perception that understanding the law is not part of their role: *“It’s not their job to understand the law. They don’t do this for their own sake. They do it for somebody”* (P.6).

Regarding resistance (n=6), lawyers also suggest two main reasons why software engineers may be reluctant to implement RDPRs. First, they are unwilling to learn and take on responsibility over it, similar to what [45] identified for ethical requirements. Second, they refuse to allocate additional resources, as it implies more work. *“So how costly it is for them to integrate data protection”* (P.38). Regarding the latter, one respondent mentioned: *“I think there is a certain resistance to trying to understand very basic concepts and recognizing that there is more to learn.”* (P.50, translated from Spanish). Similarly, another participant highlights the resistance of engineering, stating: *“there is more resistance from the computer science to accept the fact that data protection exists [...] whereas the legal part has more acceptance to deal with computer science requirements.”* (P.62). Legal professionals interpret this attitude as a lack of empathy [11]: *“They feel like their job is just to make the product and then whether it applies, like whether it complies with laws or not is a is an afterthought”* (P.14).

#### 4.3 RQ3: How do lawyers understand and fulfill their roles within interdisciplinary teams in the event of a personal data breach?

Regardless of their location, lawyers mentioned they would take similar action steps, as shown in Table 4. “Notification” (n=50) emerged as the most prominent action step, followed by “incident response” (n=43), and assessing the risk (coded as “risk of data”, n=30). According to our analysis, the majority of lawyers prioritize coordinating whom to notify, particularly supervisory authorities (n=44) and where required, affected data subjects (n=36).

Following notification duties, respondents emphasized their involvement in “incident response” activities (n=43). Finally, developing a clearer understanding of the scope and impact of the data breach was mentioned as an essential part of their role. This includes

■ **Table 4** Codes regarding interdisciplinary challenges for data protection and understanding of data protection. †: Inductive codes.

| Theme         | Code                                                    | Subcode               | Number of occurrences (percentage out of 65 interviews) |                |                   |                |                    | Total<br>n=70     |
|---------------|---------------------------------------------------------|-----------------------|---------------------------------------------------------|----------------|-------------------|----------------|--------------------|-------------------|
|               |                                                         |                       | Asia, Oceania<br>n=21                                   | Africa<br>n=10 | N. America<br>n=9 | Europe<br>n=15 | S. America<br>n=15 |                   |
| Data breaches |                                                         |                       | 17 (80.1%)                                              | 9 (90.0%)      | 6 (66.7%)         | 13 (86.7%)     | 13 (86.7%)         | <b>58 (82.9%)</b> |
|               | Notification                                            |                       | 14 (66.7%)                                              | 8 (80.0%)      | 4 (44.4%)         | 11 (73.3%)     | 13 (86.7%)         | <b>50 (71.4%)</b> |
|               |                                                         | Authority             | 13 (61.9%)                                              | 7 (70.0%)      | 3 (33.3%)         | 9 (60.0%)      | 12 (80.0%)         | <b>44 (62.9%)</b> |
|               |                                                         | Data subject          | 9 (42.9%)                                               | 5 (50.0%)      | 3 (33.3%)         | 7 (46.7%)      | 12 (80.0%)         | <b>36 (51.4%)</b> |
|               | Incident Response                                       |                       | 12 (57.1%)                                              | 9 (90.0%)      | 5 (55.5%)         | 8 (53.3%)      | 9 (60.0%)          | <b>43 (61.4%)</b> |
|               |                                                         | Containment           | 9 (42.3%)                                               | 7 (70.0%)      | 2 (22.2%)         | 4 (26.7%)      | 5 (33.3%)          | <b>27 (38.6%)</b> |
|               |                                                         | Internal Notification | 3 (14.3%)                                               | 1 (10.0%)      | 2 (22.2%)         | 0 (00.0%)      | 1 (6.7%)           | <b>7 (10.0%)</b>  |
|               | Type of Incident                                        |                       | 14 (66.7%)                                              | 7 (70.0%)      | 2 (22.2%)         | 7 (46.7%)      | 7 (46.7%)          | <b>36 (51.4%)</b> |
|               | Risk of data                                            |                       | 8 (38.1%)                                               | 4 (40.0%)      | 3 (33.3%)         | 5 (33.3%)      | 10 (66.7%)         | <b>30 (42.9%)</b> |
|               |                                                         | Type of personal data | 5 (23.8%)                                               | 2 (20.0%)      | 2 (22.2%)         | 2 (13.3%)      | 7 (46.7%)          | <b>18 (25.7%)</b> |
|               | Time                                                    |                       | 5 (23.8%)                                               | 2 (20.0%)      | 0 (00.0%)         | 5 (33.3%)      | 3 (20.0%)          | <b>15 (21.4%)</b> |
|               | Consequences (reputation)                               |                       | 5 (23.8%)                                               | 2 (20.0%)      | 1 (11.1%)         | 1 (6.7%)       | 1 (6.7%)           | <b>10 (14.3%)</b> |
|               |                                                         | Public relations      | 4 (19.1%)                                               | 0 (00.0%)      | 1 (11.1%)         | 1 (6.7%)       | 1 (6.7%)           | <b>7 (10.0%)</b>  |
|               | Interdisciplinary team<br>(legal and tech) <sup>†</sup> |                       | 2 (9.5%)                                                | 0 (00.0%)      | 3 (33.3%)         | 0 (00.0%)      | 1 (6.7%)           | <b>6 (8.6%)</b>   |

assessing the risks associated with the incident (n=30). Less frequently, respondents also brought up time constraints (n=15) and reputational consequences (n=10). An unexpected code that we created inductively was the explicit assembling an “interdisciplinary task force” (n=6).

Finding 3: Lawyers report that, in data breach cases, multiple requirements under data protection regulations are triggered. Their responses were similar across jurisdictions, highlighting the need to notify relevant actors of the breach, collaborate with incident response teams, and identify the type of breach, why it occurred, and how to mitigate it.

#### 4.3.1 Notification (50 participants)

A dominant code that emerged from the respondents’ responses regarding data breaches is notification. They mention their actions are driven by legal pressures and obligations imposed on them by regulations. At the same time, many respondents have internalized highly routinized internal escalation pathways. In the event of a data breach, they reported knowing exactly what steps to take - or at least where to find the relevant procedures. One respondent articulates this clearly: *“So I would, my first step would be to check again the legal requirements and then to act immediately”* (P.37). Participants also highlighted that notification is not a single action to authorities and data subjects, but also to internal stakeholders. One participant explains: *“Another thing I need to do is to notify our group DPO and my line manager, the head of compliance, just to give them a heads up, as well as the general counsel and the country lawyer...”* (P.22).

#### 4.3.2 Incident Response (IR) (43 participants)

After notifications, IR was the second most prominent code. Our analysis revealed that respondents described IR as a highly collaborative process that requires close coordination with technical teams. Participants emphasized that their role centers on understanding the nature of the breach and discussing containment strategies. One participant explains that IR begins with understanding *“[...] what can be immediately done to prevent further breach or incidence”* (P.8). Another participant highlights the importance of security mitigation: *“so how are you going to contain technically the impact of that breach”* (P.43).

### 4.3.3 Type of incident (36 participants)

This code was mentioned by nearly half of the participants. This typically involves understanding precisely what data has been compromised. As one participant emphasized, this process begins with understanding the basic facts, such as time, who, and “[...] *also if any personal data that, of course, belongs to you were involved in this accident* ” (P.39). This code was mentioned less frequently than the notification code, even though assessing the type of data that has been compromised is directly related to notification obligations under data protection laws, as indicated by the following quote: “*If it’s consumer data, if it’s client or people’s information, I believe then I have to approach the data protection board*” (P.15). It appears that determining the type of incident requires close collaboration between technical teams and lawyers. This collaboration is necessary in order to assess and understand risk, which informs legal actions.

## 5 Discussion and Implications

Designing compliant information systems requires the close collaboration of interdisciplinary teams with both legal and technical expertise. While prior research indicates that technical professionals struggle to understand and implement RDPRs, not enough is known about the challenges legal professionals face. Therefore, our study set out to 1) investigate the challenges that lawyers face when collaborating with technical professionals on the implementation of data protection requirements, 2) explore lawyers’ beliefs about why software engineers have difficulty understanding and implementing RDPRs, and 3) examine how lawyers understand and fulfill their roles within interdisciplinary teams in the event of a personal data breach.

By focusing on the mental models of legal professionals, our findings shed light on an understudied dimensions of RDPR implementation and offer novel insights to both scholars and practitioners. **Notably, we reveal that regardless of their jurisdiction, lawyers share similar experiences, perceptions and role identities when in interdisciplinary teams, such as a lack of common language, different mental models, communication issues, and a lack of technical education.** Some of the findings of our work align with previous findings from studies focusing on software engineers [23], now providing the complementary perspective, that of legal experts. **Our findings have several practical implications for requirements and privacy engineers worldwide, which we will discuss in more detail below.**

### 5.1 Global experiences of legal experts

Legal experts across jurisdictions shared similar experiences, suggesting that these are jurisdiction-independent. The development of artifacts that facilitate collaboration between software engineers and lawyers on RDPRs can also be jurisdiction-independent.

Throughout our analysis, participants consistently reported similar experiences when collaborating in interdisciplinary teams. Their experiences converged around common challenges and perceptions, particularly the widespread belief that software engineers lack a shared understanding of RDPRs with legal experts. These patterns appear to be independent of jurisdiction, legal culture, or enforcement, indicating a recurring phenomenon across countries.

A shared understanding is fundamental to conceptualize RDPRs [46, 42, 19]. Regardless of specific regulations, most participants agree that software engineers’ conceptualizations impede their understanding of data protection. This observation raises questions about the

prevalence of this phenomenon. Legal experts further reported they would react similarly to a data breach, regardless of jurisdiction. The fact that most participants would notify and then call for incident response to identify the type of incident and the risk to data shows how standardized the response to (personal) data breaches is worldwide. This is not a surprising finding given the cybersecurity standardization efforts. While jurisdictions may differ, legal experts' experiences collaborating with software engineers are similar. Therefore, future work could focus on developing artifacts that are jurisdiction-agnostic and can work in different national contexts.

## 5.2 Communication is not about vocabulary

The RDPRs collaboration problem is not one of natural language per se, but rather the meaning of the terms: lawyers and software engineers often use the same terms with different conceptualizations, as they have different mental models resulting from education and incentives. Legal experts highlight that conceptualizing RDPRs requires legal knowledge beyond a single regulation, including an understanding of its legal foundations.

Our findings highlight that between lawyers and engineers, the problems of communication are not about language, but about conceptualization. As explained in the results, differences in mental models show that oftentimes both sides use the same words with different meanings. Hence, developing a shared understanding is critical [19]. A share of the participants believe the problems in understanding are not necessarily about the education engineers have or lack. They believe it is rather motivated by the differences in understanding of what data protection entails.

In this regard, previous literature [23] has pointed out that one of the problems for engineers to implement privacy requirements was that they apply the vocabulary of security to data protection, but these are not the same, nor do they have the same meaning or implications.

It seems that collaboration in cybersecurity is often smoother than in data protection. One possible reason we hypothesize for this is that many data protection requirements originate primarily from legal documents rather than technical standards or specifications. By contrast, cybersecurity standards are more actively developed and promoted by industry stakeholders, which may make them easier to operationalize in practice [16, 38]. That being said, during data breaches, legal experts understand their role and report smooth collaborations, which shows that communication can be facilitated through standardization and procedural clarity, or even through artifact creation, as discussed below.

## 5.3 The usage of artifacts

Teams require structured mechanisms and/or artifacts to translate context-dependent legal reasoning into implementable design constraints. Otherwise, divergent expectations regarding ambiguity and specificity hinder alignment on what compliance requires in practice. These artifacts need to be explicitly designed to accommodate the interpretive and context-dependent nature of legal reasoning in RDPR work.

Consistent with prior research in RE, this study provides additional evidence for the necessity of a shared language and understanding [19, 22, 21]. In RE, the pursuit of shared understanding underpins the development of artifacts, such as taxonomies, ontologies, and conceptual models [48]. This study also provides empirical evidence supporting the need to validate and implement RE tools for data protection in practical settings. Although multiple ontologies, vocabularies, conceptual modeling frameworks, and others exist to help establish

shared understanding, 46 of our participants (code “lack of common language”- 65.7%) still mentioned struggling with communication. Given that only 2 participants referred to intermediary modeling artifacts, we infer that the artifacts being developed are not being adopted by lawyers.

Although we do not have data to know why lawyers are not adopting these tools, we propose several hypotheses. First, lawyers may be unaware of these intermediary artifacts, suggesting a need for further dissemination. Second, these tools may not adequately capture the needs and expectations of lawyers and diminish their perceived utility to this end-user group; involving lawyers in the artifact’s development could help with this. Thus, these artifacts may primarily focus on software engineers’ needs, limiting their usefulness to lawyers and RDPRs as a whole. Future work could focus on analyzing these hypotheses and determining why this lack of adoption exists.

If new artifacts are built or adapted to deal with RDPRs, they should prioritize requirements conceptualization as complex socio-technical issues, going beyond the more classical RE functional vs. non-functional requirements conceptualization. The majority of participants emphasized the complexity of translating RDPRs into software specifications, noting the importance of having both legal and technical knowledge. We hypothesize that RDPRs encompass elements from business processes, strategic objectives, technical considerations, privacy-enhancing technologies, and human rights, among others. Oversimplifying RDPRs risks neglecting their complexity, leading to an ill-designed IS. Thus we propose that data protection requirements should constitute a distinct domain within RE, similarly to security requirements.

## 5.4 The role of empathy in privacy requirements engineering

Interdisciplinary data protection teams are hindered by asymmetries in legal and technical expertise and the absence of a shared language. Thus, effective collaboration requires organizational strategies that include legal experts, and that foster mutual understanding, cross-disciplinary knowledge, and inclusive privacy practices.

With this study, we also provide further evidence of the struggles faced by interdisciplinary data protection teams. Lawyers perceived interdisciplinary teams to struggle due to a lack of shared language, the need for a better understanding of the nuances and complexity of regulations among engineers and technical knowledge among lawyers. Any attempt at supporting the communication between lawyers and engineers needs to consider this.

Promoting communication and unified understanding requires improving organizational privacy culture [43]. Our results point to the need to also include lawyers in the process. In this regard, [26] talk about the need to develop empathy among stakeholders to motivate engineers to implement privacy. In light of our results, this could be a potential approach since lawyers also see themselves as lacking knowledge/education, and value engineers’ expertise as necessary for resolving privacy issues (e.g., data privacy breaches). Approaching interdisciplinary collaborations among stakeholders in organizations is a promising approach that is being studied in other domains, such as user experience and service design, where it has been proven useful for improving service quality through a stronger user-centered approach [12].

## 6 Threats to validity and limitations

While our study provides valuable insights into the mental models of lawyers who work or have worked with software engineers on data protection for IS, we also acknowledge three main limitations that present opportunities for future research. First, although our sample included lawyers from 25 countries and covered most G20 economies as well as other jurisdictions. Certain regions, including Oceania and parts of Eastern Europe, were underrepresented. Limiting recruitment to G20 economies and the number of additional invitees was necessary due to time and resource limitations. Russia was excluded due to sanctions in place at the time of ethical approval. Future studies should therefore expand the sample size by reaching out to participants from underrepresented regions to complement our findings with these additional perspectives.

Second, the present study relies on interview data, which is susceptible to various forms of bias. For example, participants' accounts may have been influenced by social desirability, causing them to present themselves or their profession in a more favorable light. To mitigate this risk, we built rapport with the participants prior to the interviews. Additionally, we informed all participants that there were no right or wrong answers and that "I don't know" was a valid and interesting response. Furthermore, as participation was voluntary and non-remunerated, self-selection bias may have influenced the findings.

Another limitation involves the way lawyers conceptualize various stakeholders. Participants referred to 'computer scientists, programmers, or [verbatim] "you guys" (referring to software engineering) when describing the technical stakeholders with whom they interact. This limitation restricts the ability to distinguish among software engineers, architects, incident response personnel, and other technical roles in the analysis. As a result, these roles are grouped together, despite differences in responsibilities and expertise. Future research could investigate whether lawyers' experiences vary regarding specific roles within computer science.

Our deductive approach was well-suited to answering our research questions but may have limited our ability to identify new codes that fell outside the defined topics. The authors' diverse academic and professional backgrounds, spanning computer science, economics, engineering, informatics, law, political science, and psychology, enriched but may have also influenced the analysis. To mitigate bias, we therefore implemented multiple validation steps: the initial codebook was reviewed by five independent lawyers from different jurisdictions (EU, Chile, Brazil, and China). Next, the authors conducted several calibration sessions. Finally, all interviews were double-coded by two researchers and disagreements resolved through discussion. To enhance transparency and reproducibility, we provide detailed methodological documentation; however, interpretive subjectivity remains inherent to qualitative studies [27].

To increase both the transparency and trustworthiness of this study, we provide as much data and details as possible within the paper [41]. However, due to space limitation, specific details and documents are not included here but made available in the public repository [41].

## 7 Conclusion

This paper presents a global overview of lawyers' experiences collaborating with software engineers on regulatory data protection requirements, drawing on a qualitative deductive analysis of 70 interviews. Their experiences are consistent across regions and converge on three primary challenges: lack of shared understanding, difficulties in comprehending regulatory data protection, and insufficient empathy. Legal experts generally do not employ intermediary artifacts to facilitate common ground or serve as communication tools. In the context of data breaches, however, their roles are well-defined, and the processes for managing such events are becoming increasingly standardized worldwide.

Our results imply that it is not just “natural language” that hinders collaboration between lawyers and software engineers, but also their underlying conceptualizations. Although multiple artifacts from the requirements engineering community have been proposed, they appear not to accommodate the needs and legal reasoning of regulatory data protection requirements. These results and implications have important consequences, as they stress the globally shared experience of lawyers when dealing with these types of requirements.

## 8 Data Availability Statement

Due to the qualitative nature of this study and respecting the consent and privacy of the participants, not all interviews can be shared. Some are available in the Zenodo repository DOI 10.5281/zenodo.15166882 or upon request of the leading author, depending on the consent. In order to provide maximum transparency, we provide other materials in the repository, such as the codebook, interview questions, and other material deemed relevant.

## 9 AI usage in this paper

This article has used a paid version of Grammarly to correct and fix spelling mistakes. The codes definition in the codebook was written by the author, and they used Grammarly and Chat GPT 4.0 for identifying spelling and grammar mistakes. If consented by the participant, interviews were transcribed using AIKO, which was then proof-read and corrected to ensure accuracy of the transcription. The authors have no other disclaimer on the usage of AI.

---

## References

- 1 Simone Agostinelli, Fabrizio Maria Maggi, Andrea Marrella, and Francesco Sapio. Achieving gdpr compliance of bpmn process models. In *Information Systems Engineering in Responsible Information Systems: CAiSE Forum 2019, Rome, Italy, Proceedings 31*. Springer, 2019.
- 2 Vanessa Ayala-Rivera and Liliana Pasquale. The grace period has ended: An approach to operationalize gdpr requirements. In *2018 IEEE 26th International Requirements Engineering Conference (RE)*, pages 136–146, 2018. doi:10.1109/RE.2018.00023.
- 3 Earl R Babbie. *The practice of social research*. Cengage learning, 2020.
- 4 Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. Engineering privacy by design: Are engineers ready to live up to the challenge? *The Information Society*, 35(3):122–142, 2019. doi:10.1080/01972243.2019.1583296.
- 5 Andrea J Bingham. From data management to actionable findings: A five-phase process of qualitative data analysis. *International journal of qualitative methods*, 22:16094069231183620, 2023.
- 6 Anu Bradford. *The Brussels effect: How the European Union rules the world*. Oxford University Press, 2020.
- 7 Travis Breaux and Annie Antón. Analyzing regulatory rules for privacy and security requirements. *IEEE transactions on software engineering*, 34(1):5–20, 2008. doi:10.1109/TSE.2007.70746.
- 8 Travis Breaux and Thomas Norton. Legal accountability as software quality: A u.s. data processing perspective. In *International Requirements Engineering Conference (RE)*. IEEE, 2022.
- 9 Travis D Breaux and Annie I Antón. A systematic method for acquiring regulatory requirements: A frame-based approach. *RHAS-6, Delhi, India*, 2007.
- 10 Daniela Damian and James Chisan. An empirical study of the complex relationships between requirements engineering processes and other processes that lead to payoffs in productivity, quality, and risk management. *IEEE Trans. Software Eng.*, 32:433–453, July 2006. doi:10.1109/TSE.2006.61.

- 11 Kezia Devathasan, Nowshin Nawar Arony, Emerson Murphy-Hill, and Daniela Damian. Empathy, self-determination and motivation: moderating diversity for enhanced performance in software development teams. *Empirical Software Engineering*, 30(3):82, 2025. doi:10.1007/S10664-025-10632-2.
- 12 Luce Drouet, Froukje Sleeswijk Visser, Brian Pagán, and Carine Lallemand. Towards a mapping of empathic design methods. In *DRS Conference Proceedings*. Design Research Society, 2024.
- 13 Eduarda Elger and Victor Araya Santander. A engenharia de requisitos e a lei geral de proteção de dados (lgpd): Uma revisão sistemática da literatura. In *Congresso Latino-Americano de Software Livre e Tecnologias Abertas (Latinoware)*, pages 1–10. SBC, 2024.
- 14 European Union. Regulation (EU) 2016/678 of the european parliament and of the council - general data protection regulation.
- 15 Stephen T Fife and Jacob D Gossner. Deductive qualitative analysis: Evaluating, expanding, and refining theory. *International Journal of Qualitative Methods*, 23:16094069241244856, 2024.
- 16 Adebola Folorunso, Viqaruddin Mohammed, Ifeoluwa Wada, and Bunmi Samuel. The impact of iso security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, 24(1):2582–2595, 2024.
- 17 Raphaël Gellert and Serge Gutwirth. The legal construction of privacy and data protection. *Computer Law & Security Review*, 29(5):522–530, 2013. doi:10.1016/J.CLSR.2013.07.005.
- 18 Mohamad Gharib, Paolo Giorgini, and John Mylopoulos. Ontologies for privacy requirements engineering: A systematic literature review. *arXiv preprint arXiv:1611.10097*, 2016. arXiv:1611.10097.
- 19 Martin Glinz and Samuel A Fricker. On shared understanding in software engineering: an essay. *Computer Science-Research and Development*, 30:363–376, 2015. doi:10.1007/S00450-014-0256-X.
- 20 Geetika Gopi, Aadyaa Maddi, Omkhar Arasaratnam, and Giulia Fanti. Privacy requirements and realities of digital public goods. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 159–177, 2024. URL: <https://www.usenix.org/conference/soups2024/presentation/gopi>.
- 21 Giancarlo Guizzardi and Nicola Guarino. Explanation, semantics, and ontology. *Data & Knowledge Engineering*, page 102325, 2024. doi:10.1016/J.DATAK.2024.102325.
- 22 Giancarlo Guizzardi, Gerd Wagner, João Paulo Andrade Almeida, and Renata SS Guizzardi. Towards ontological foundations for conceptual modeling: The unified foundational ontology (ufo) story. *Applied ontology*, 10(3-4):259–271, 2015. doi:10.3233/A0-150157.
- 23 Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. Privacy by designers: software developers’ privacy mindset. *Empirical Software Engineering*, 23(1):259–289, 2018. doi:10.1007/S10664-017-9517-1.
- 24 Kalle Hjerppe, Jukka Ruohonen, and Ville Leppanen. The general data protection regulation: Requirements, architectures, and constraints. In *2019 IEEE 27th International Requirements Engineering Conference (RE)*, pages 265–275. IEEE, September 2019. doi:10.1109/RE.2019.00036.
- 25 Oleksandra Klymenko, Oleksandr Kosenkov, Stephen Meisenbacher, Parisa Elahidoost, Daniel Mendez, and Florian Matthes. Understanding the implementation of technical measures in the process of data privacy compliance: A qualitative study. In *Proceedings of the 16th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM ’22*, pages 261–271, New York, NY, USA, 2022. Association for Computing Machinery. doi:10.1145/3544902.3546234.
- 26 Meira Levy and Irit Hadar. The importance of empathy for analyzing privacy requirements. In *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, pages 9–13, August 2018. doi:10.1109/ESPRE.2018.00008.

- 27 Katja Mruck and Franz Breuer. Subjectivity and reflexivity in qualitative research – a new fqs issue. *Historical Social Research*, 28(3):189–212, 2003. doi:10.12759/hsr.28.2003.3.189–212.
- 28 Claudia Negri-Ribalta, Marius Lombard-Platet, and Camille Salinesi. Understanding the gdpr from a requirements engineering perspective—a systematic mapping study on regulatory data protection requirements. *Requirements Engineering*, pages 1–27, 2024.
- 29 Claudia Negri-Ribalta, Rene Noel, Oscar Pastor, and Camille Salinesi. An empirical study on socio-technical modeling for interdisciplinary privacy requirements. In *CoopIS*. Springer, 2023.
- 30 Leysan Nurgalieva, Alisa Frik, and Gavin Doherty. A narrative review of factors affecting the implementation of privacy and security practices in software development. *ACM Comput. Surv.*, 55(14s):320:1–320:27, July 2023. doi:10.1145/3589951.
- 31 Klaus Pohl. *Requirements engineering: fundamentals, principles, and techniques*. Springer Publishing Company, Incorporated, 2010.
- 32 Maxwell Prybylo, Sara Haghighi, Sai Teja Peddinti, and Sepideh Ghanavati. Evaluating privacy perceptions, experience, and behavior of software development teams. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 101–120, 2024. URL: <https://www.usenix.org/conference/soups2024/presentation/ prybylo>.
- 33 Rivka Ribak. Translating privacy: developer cultures in the global world of practice. *Information, Communication & Society*, 22(6):838–853, May 2019. doi:10.1080/1369118X.2019.1577475.
- 34 Marco Robol, Mattia Salnitri, and Paolo Giorgini. Toward gdpr-compliant socio-technical systems: modeling language and reasoning framework. In *IFIP Working Conference on The Practice of Enterprise Modeling*, pages 236–250. Springer, 2017. doi:10.1007/978-3-319-70241-4\_16.
- 35 Awanthika Senarath and Nalin A. G. Arachchilage. Why developers cannot embed privacy into software systems? an empirical investigation. In *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018, EASE’18*, pages 211–216, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3210459.3210484.
- 36 Swapneel Sheth, Gail Kaiser, and Walid Maalej. Us and them: A study of privacy requirements across north america, asia, and europe. In *Proceedings of the 36th International Conference on Software Engineering, ICSE 2014*, pages 859–870, New York, NY, USA, 2014. Association for Computing Machinery. doi:10.1145/2568225.2568244.
- 37 Martina Siclari, Sylvain Lannier, Olivier Voordeckers, Stanislaw Tosza, Sallam Abualhaija, Michele Ceci, Nicolas Sannier, and Domenico Bianculli. Beyond silos: Bridging the gap between law and software engineering – challenges, successes, and lesson drawing. *Internet Policy Review*, 14(4), 2025. doi:10.14763/2025.4.2042.
- 38 Hardial Singh. The importance of cybersecurity frameworks and constant audits for identifying gaps, meeting regulatory and compliance standards. In *Meeting Regulatory and Compliance Standards (November 10, 2022)*, 2022.
- 39 Daniel J Solove. A taxonomy of privacy. *University of Pennsylvania law review*, 2006.
- 40 Sarah Spiekermann, Jana Korunovska, and Marc Langheinrich. Inside the organization: Why privacy and security engineering is a challenge for engineers. *Proceedings of the IEEE*, 107(3):600–615, March 2019. doi:10.1109/JPROC.2018.2866769.
- 41 Per Erik Strandberg. Ethical interviews in software engineering. In *2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, pages 1–11. IEEE, 2019. doi:10.1109/ESEM.2019.8870192.
- 42 Alistair Sutcliffe. Collaborative requirements engineering: bridging the gulfs between worlds. In *Intentional Perspectives on Information Systems Engineering*, pages 355–376. Springer, 2010. doi:10.1007/978-3-642-12544-7\_20.

- 43    Mohammad Tahaei, Alisa Frik, and Kami Vaniea. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pages 1–15, New York, NY, USA, May 2021. Association for Computing Machinery. doi:10.1145/3411764.3445768.
- 44    Damiano Torre, Mauricio Alferez, Ghanem Soltana, Mehrdad Sabetzadeh, and Lionel Briand. Modeling data protection and privacy: application and experience with gdpr. *Software and Systems Modeling*, 20:2071–2087, 2021. doi:10.1007/S10270-021-00935-5.
- 45    Ibo Van de Poel. Investigating ethical issues in engineering design. *Science and engineering ethics*, 7(3):429–446, 2001.
- 46    Colin Werner, Laura Okpara, Klaas-Jan Stol, and Daniela Damian. Maintaining shared understanding of non-functional requirements in small companies using continuous software engineering. *Empirical Software Engineering*, 31(2):40, 2026. doi:10.1007/S10664-025-10765-4.
- 47    A.F. Westin and D.J. Solove. *Privacy and Freedom*. Ig Publishing, 2015.
- 48    Roel J Wieringa. *Design science methodology for information systems and software engineering*. Springer, Berlin, Heidelberg, 2014. doi:10.1007/978-3-662-43839-8.