“Those things are written by lawyers, and programmers are reading that.” Mapping the Communication Gap Between Software Developers and Privacy Experts

Stefan Albert Horstmann
Ruhr University Bochum

Samuel Domiks
Independent

Marco Gutfleisch
Ruhr University Bochum

Mindy Tran
Paderborn University

Yasemin Acar
The George Washington University &
Paderborn University

Veelasha Moonsamy
Ruhr University Bochum

Alena Naiakshina
Ruhr University Bochum

ABSTRACT

To ensure data-privacy compliance, it is common for companies to consult privacy experts for the identification and communication of privacy requirements to software developers. However, developers often fail to fulfill those requirements resulting in companies regularly being fined for violations due to non-compliance with privacy data regulations. To investigate why software developers struggle with the implementation of privacy requirements and explore their communication modality, we conducted a qualitative semi-structured interview study with 30 participants involving 10 software developers, 10 privacy experts, and 10 team coordinators with an average experience of nine years in the privacy communication and implementation process within a company context. We found a communication gap between software developers and privacy experts, suggesting a lack of proper procedural steps during the software development process to guarantee that the privacy requirements have been adequately addressed. We also uncovered that since privacy requirements were mostly communicated in a uni-directional manner, they were often perceived as a hindrance during software development, thus fostering an adversarial relationship between privacy experts and developers. Therefore, in order to fulfill the experts’ requirements, software developers requested concrete steps to take during the software development process, as observed in the security field. However, privacy experts often lacked the technical knowledge to provide such instructions. This work contributes an explanatory theory on the communication gap between software developers and privacy experts. We discuss common obstacles in the communication of privacy experts and software developers and provide guidance on how to address them.

Proceedings on Privacy Enhancing Technologies 2024(1), 151–170

https://doi.org/10.56553/popets-2024-0010

KEYWORDS

privacy, privacy requirements, software engineering, GDPR, CCPA, communication, qualitative research

1 INTRODUCTION

Since the implementation of the General Data Protection Regulation (GDPR) in May 2018, at least 1300 fines (as of November 2022 [31]) have been issued for violations or non-compliance. Five years and over two billion euros in fines later [31], software developers still struggle with implementing privacy requirements [14, 46, 47, 68, 72, 89, 95]. During the software development process, the burden of implementing those requirements is often placed on developers who are rarely privacy experts and are confronted with challenges related to implementation [14, 47, 68, 89]. This motivated a line of privacy research investigating software developers’ behavior with privacy tasks (e.g., [5, 6, 46, 47, 64, 73, 82, 85, 86, 89]). To improve data-privacy compliance, companies are advised to hire or consult privacy experts who can translate regulations into privacy requirements for software products. For this work, we define privacy experts as individuals with a high level of knowledge or skill in data protection law and data privacy practices, e.g., by having a legal background or acting as a privacy specialist [17, 58]. While privacy experts can have the role of data protection officers (DPO) [23], they can also act as privacy consultants, e.g., for the Information Commissioner’s Office (ICO) [55].

In this paper, we explored why software developers struggle to implement privacy requirements, focusing on the communication process between development teams and privacy experts. We conducted 30 semi-structured interviews with software developers, privacy experts, and team coordinators using Grounded Theory [18]. Due to lack of time, spread out geographical locations, and high cost [2–4, 40, 44, 45, 76, 102], it is challenging to recruit software developers, specifically in the field of security and privacy research [1, 28, 44, 54, 74, 87]. We opted for an international sample experienced in different regulations to investigate privacy requirements relevant to a global context. Thus, based on previous research recommendations exploring different recruitment samples, methods, and platforms [39, 69], we recruited a cross-section of participants from various locations with expertise in software development and privacy on Upwork.com [93]. Theoretical sampling indicated that employees with team coordinator positions (e.g., team leads, product owners) in software development teams play a crucial role in the communication process, henceforth referred to as team coordinators. The online interviews were conducted via Zoom [24] and lasted 57 minutes on average and 28.6 hours in total. To provide deeper insights into the privacy practices and issues faced by parties involved in the communication of privacy requirements, we investigated the following research questions:

RQ1: "*What are developers', team coordinators', and privacy experts' perceptions of privacy requirements?*"
RQ2: "*How does the communication of privacy requirements between developers, team coordinators, and privacy experts look like?*"
RQ3: "*How do privacy experts create, and team coordinators and developers implement privacy requirements?*"

We provide the results of an exploratory qualitative study to understand how software developers and privacy experts perceive, communicate and implement privacy requirements within a company context. Our key insights are as follows:

- **Adversarial relationship**: Developers often consider privacy requirements restrictive and hard to comprehend, resulting in an adversarial attitude towards experts providing these requirements.
- **Team coordinators**: We found that communication between developers and privacy experts is almost non-existent and often indirect. Team coordinators play a critical role in acting as the pivot point for privacy-related communication. Further, individual developers might take responsibility for privacy requirements as privacy champions within the development team.
- **Differentiating between security and privacy**: Supporting the findings of Hadar et al. [11], we found the distinction between *security* and *privacy* terminologies was often unclear on the development side.
- **Lack of privacy requirements verification**: We found that verifying the implementation of privacy requirements is not a standard procedure within the companies our participants worked for.

Contributions. With this work, we contribute an explanatory theory on the communication gap between privacy experts and software developers grounded in the data collected from our participants. We highlight common obstacles in the communication of privacy experts and developers, discuss how to address them, and provide guidance on embedding privacy principles into the software development process.

2 RELATED WORK

This section summarizes related work focusing on the effect of introduced data protection regulations, the resulting challenges software developers face in implementing privacy requirements, and their behavior in regard to privacy compliance tasks.

Data protection regulation. The introduction of data protection regulation was studied broadly in the past [43, 92, 94]. In 2018, Sirur et al. [75] studied how companies evaluated the introduction of GDPR and how prepared they were for this regulatory change. While some companies reported being prepared, others seemed to face difficulties keeping up with the legislation unless they strongly focused on security and privacy. Von Davier et al. [103] conducted an interview study with eight privacy professionals and found participants having issues with translating legislation into practice and the unclear job description of a DPO. They concluded that promoting the importance of privacy in companies is still necessary. Further research analyzed the causes of GDPR fines [49, 68], showing human error and organizational issues as potential causes. There seem to be many layers of confusion within organizations. Therefore, exploring how different perceptions about privacy concepts manifest in corporations is crucial.

Challenges of implementing privacy requirements. Senarath et al. [72] conducted a study with 36 developers to identify challenges from embedding privacy requirements into software applications. They found developers lack formal knowledge of privacy practices such as Privacy by Design (PbD), Fair Information Practices (FIP), Data Minimization (DM), and Privacy Impact Assessment (PIA). Similarly, the studies conducted by Alhazmi et al. [5, 6] examined the reasons preventing developers from adopting GDPR principles in their applications and software systems. They reported the focus on functional requirements, a lack of knowledge of GDPR principles, and supporting online tools as the main challenges faced by developers.

The research conducted by Tahaei et al. [82, 85, 86, 89] showed that developers mainly face challenges when writing and modifying privacy policies, working or designing systems with access control, dealing with updates to platforms and APIs, and deciding on the privacy aspects of their projects. Further, they found that a negative privacy culture, disparate internal prioritization, missing tools, metrics, and high technical complexity pose barriers to implementing privacy – also observed in [64]. Participants in the studies mentioned that informal discussions, strong support and communication from management and stakeholders, and documentation and guidelines helped promote privacy. Further, code reviews and practical training seem useful.

Research on websites' privacy notifications and cookie policies [26, 48, 79, 96, 97], as well as privacy information from apps [41, 47, 80] showed that software developers and companies were often unable to create notifications accurately. Further challenges were identified by analyzing general compliance to the legislation of apps [7, 70] and monitoring conversations on privacy in online developer forums [63, 84]. For example, developers faced issues keeping track of the data collected by their application, often through third-party libraries, and thus struggled to provide accurate information for their users.

Developers' attitudes towards privacy adoption. Ayalon et al. [11] conducted an online survey with 101 developers to study their privacy decision-making processes. They investigated whether organizational, professional, or personal factors shape developers' privacy decision-making. They found that personal experiences as end users, organizational privacy climate, and compatibility with existing frameworks play a vital role in their decision-making. These findings align with Hadar et al.'s [36] interview study, adding that developers often confound data security with privacy challenges, thus limiting their perceived privacy threats.

Van der Linden et al. [98] conducted a study with 123 software developers to examine their attitude towards handling personal data, specifically, how concerned they are about privacy in the software development context. They found a mismatch between developers' attitudes and their self-perceived behavior. Further, developers' understanding of appropriate data collection and privacy principles and laws seemed to differ substantially.

The work of Balebako et al. [12] offered further insights into how mobile app developers make decisions relating to privacy and security, and examined the correlation between privacy and security behavior and characteristics of app development companies. They found that small companies were less likely to demonstrate good privacy and security behavior and that developers were often unaware of the vast amount of invasive data being collected by third-party tools.

Bednar et al. [14] interviewed six senior engineers to investigate their motivation and ability to comply with privacy regulations. They found that engineers believe privacy is a legal issue for which the legal world is responsible by providing legal frameworks and guidelines. There seemed to be a lack of perceived responsibility, control, autonomy, and frustration in interacting with the legal world.

In summary, past research showed that software developers often lack knowledge and have difficulties fulfilling privacy requirements. Therefore, they often do not implement or favor poor practices to ensure data privacy. While existing research suggests communication issues of privacy requirements, no research has been conducted yet to explore these with software developers and privacy experts. Our work complements and extends the growing line of privacy research with developers by examining the privacy requirements communication and implementation process between privacy experts, developers, and team coordinators.

3 METHODOLOGY

To provide insights into the collaboration of privacy experts and software developers, we conducted semi-structured interviews with 30 participants involved in communicating and implementing privacy requirements within a company context.

We were not aware of previous research on the communication between software developers and privacy experts. However, we had previous knowledge of data protection regulations and privacy-related research with software developers. Therefore, we used Grounded Theory by Charmaz [18, 19] as the methodology for our qualitative research allowing an *"in-depth exploration of a particular topic"* [18] by *"recognizing prior knowledge and theoretical preconceptions"* [19]. We recruited our participants online via Upwork [93] and asked them to fill out a short screening questionnaire, ensuring they were involved in communicating and implementing privacy requirements and had experience with privacy expert and developer collaborations. Participants fulfilling the requirements were asked to complete a questionnaire on their demographics and were invited to the interview study. All 30 interviews were conducted in English by the same researcher using the video communications platform, Zoom [24]. Interviews lasted 57 minutes on average. The questionnaires and the interview guideline can be found in the supplementary material.

3.1 Interview Guideline

The semi-structured interview guideline consisted of three main parts. First (see Section 4.1), we were interested in how participants perceived privacy requirements. For this, we asked them to explain common privacy concepts software developers are most familiar with but often lack knowledge of, as suggested by Senarath and Arachchilage in [72]: Privacy by Design (PbD), Privacy Impact Assessment (PIA), Fair Information Practices (FIP), and Data Minimization (DM). We also asked for their experience with privacy concepts within the work context. Second (see Section 4.2), we asked participants about their role within the company, the company context, and how privacy requirements are implemented in the software development process (e.g., Who creates the privacy requirements? Who is responsible for ensuring that the privacy requirements are implemented? Do they understand the requirements?). We were specifically interested in communication processes between privacy experts and software developers.

Third (see Section 4.3), we presented participants with concrete privacy requirement tasks inspired by several blog posts (e.g., [32, 52, 71]) and asked for *"think-aloud"* walkthroughs. The tasks included technical examples for enabling access control for a hypothetical database and ensuring a maximum time for data retention. Further, collected data should not be used for advertising purposes. We contacted a commercial company involving software developers and privacy experts and approved that these were real-life examples the groups are often confronted with. Participants often referred to security practices when asked about privacy requirements within the first batches of interviews (9 with developers, 5 with privacy experts, and 5 with team coordinators). Since using grounded theory strategies allowed us to respond to new insights [19], we clarified that we were not asking for data security and provided data protection and data privacy definitions within the following interviews, according to GDPR [57, 62]. Data protection means "keeping data safe from unauthorized access" [57]. Data protection principles are defined in Chapter 2 (Art. 5-11) [59] of the GDPR. For example, in the context of data minimization, it should be collected and processed only as much data as absolutely necessary for the purposes specified (see Art. 5(1)(c) [59]). Data privacy means "empowering your users to make their own decisions about who can process their data and for what purpose" [57]. Data privacy rights of the data subject are defined in Chapter 3 (Art. 12-23) [60] of the GDPR. We clarified we were not asking about data security according to [62] where "you're required to handle data securely by implementing appropriate technical and organizational measures" [61]. However, we did not observe an effect of providing the definitions since we reached theoretical saturation between the 23rd and 25th interviews, i.e., no new properties emerged in interviews 25-30 (see Section 3.3). The final interview guideline can be found in the supplementary material.

Table 1: Participants' demographics.

Gender					
Male	25	83.3%	Prefer not to answer	1	3.3%
Female	4	13.3%			
Countries					
India	6	20.0%	UK	4	13.3%
United States	4	13.3%	Other	13	43.3%
Kenya	3	10.0%			
Age [years]					
Min.	23		Max.	44	
Mean (Std.)	33.6	±5.5	Median	33	
Industry Experience [years]					
Min.	0.5		Max.	20	
Mean (Std.)	9.1	±4.5	Median	8.5	
Domain Experience [years]					
Min.	3		Max.	19	
Mean (Std.)	8.25	±4.11	Median	8	
Education					
Bachelor's degree	10	33.3%	Graduate school	3	10.0%
College	1	3.3%	Master's degree	12	40.0%
Vocational degree	1	3.3%	Doctorate / PhD	3	10.0%
Current Employment Status					
Employed, full-time	18	60%	Employed, part-time	3	10.0%
Self-Employed	7	23.33%	Prefer not to say	2	6.67%
Largest Company Size (Employees)					
Min.	2		Max.	400000	
Mean (Std.)	41996	±99633	Median	350	
No Answer: 4					

3.2 Recruitment and Demographics

We recruited participants on Upwork.com [93], where software developers and privacy experts offer their services as freelancers. Participants were invited to take part in a short screening questionnaire asking for experience with communicating and implementing privacy requirements. Forty-eight participants filled out the screening questionnaire, of whom 34 participants were invited to the study. The 14 participants not invited to the study either did not fit the requirements (e.g., not having received or created privacy requirements in the past), expected higher compensation, or stopped replying to messages. Thirty-two participants completed the demographics questionnaire. One participant dropped out after filling out the demographics survey and was not interviewed. Out of 31 interviews, one was removed from analysis due to audio issues, leaving us with 30 interviews used for analysis. Participation was compensated with $75 via Upwork. Recruitment took place from September to November 2022.

The aggregated demographics of our participants can be found in Table 1 and participants' job titles in Table 2. We recruited 10 software developers, 10 privacy experts, and 10 team coordinators. Participants were from 16 countries, including India (6), USA (4), UK (4), Kenya (3), Belgium (2), etc. Most of our participants were male (25 male, 4 female, 1 prefer not to answer). They were, on average, 33.5 years old (min: 23, med: 33, max: 44), with an average of 9.1 years of industry experience (min: 0.5 med: 8.5, max: 20). Most had a Master (12) or a Bachelor (10) as their highest degree. Three participants had finished graduate school, and three others had a doctorate or PhD. Seven participants worked for companies with less than 100 employees, 9 worked for companies with 100 to 1000 employees, and 10 worked for companies with more than 1000 employees.

Table 2: Participants' job title

Participant	Current Job Title
D1	Technical Lead
D2	Web developer & Compliance Freelancer
D3	Chief Technology Officer
D4	Backend software developer
D5	Chief Digital Officer
D6	Software & IT Consultant
D7	Software Developer
D8	Senior Software Developer
D9	Freelance Software Developer
D10	FullStack Engineer
E1	Legal Coordinator and DPO
E2	Managing Director
E3	Security & Privacy Officer
E4	Legal advisor in the field of privacy
E5	Director of Cybersecurity and Data Privacy
E6	CISO
E7	Privacy Officer and Privacy Counsel
E8	Data Protection Officer / Privacy Specialist
E9	Barrister / Tech Contract Specialist Lawyer
E10	Legal Specialist
C1	Product Director
C2	Technical Project Manager
C3	Sr Software Engineer
C4	Group Product Manager
C5	Transformation Program Manager
C6	CEO
C7	Product Owner
C8	Technical Project Manager
C9	CEO
C10	Product management consultant

D= Software Developer, E= Privacy Expert, C= Team Coordinator

3.3 Data Analysis

For data analysis, we used the core concepts of the *constructivist approach* by Charmaz [18] consisting of (1) initial coding: incident-by-incident, (2) focused coding: selecting categories from the essential codes, and (3) theoretical coding: specifying relationships between categories [78]. Theoretical sampling advocates for *"seeking and collecting pertinent data to elaborate and refine categories [...] until no new properties emerge"*, i.e., theoretical saturation is reached [18]. In our interviews, participants often referred to team leads, project managers, or software developers in similar positions to be responsible for communicating privacy requirements. After conducting five interviews with developers and privacy experts each, we specifically invited team coordinators (see Table 2) involved in sharing privacy requirements with the software development teams to further elaborate the categories *"Exchanged Information," "Communication Challenges,"* and *"Communication Good Practices."* Participants D2-D5 and E1-E5 mentioned this group being more directly involved in the communication process. Thus, our final sample involved privacy experts, software developers, and team coordinators.

The interviews were transcribed and analyzed by three researchers (R1, R2, R3) involved in this work. After coding the first four interviews individually, the three researchers developed one codebook (see Appendix E) for all three groups due to overlapping codes between the three roles. Disagreements were resolved by discussion, e.g., if code terms were similar in meaning but differed in wording (e.g., "tracking" and "cookies"), one common code was used. If code terms were similar in wording but different in meaning (e.g., differentiating between in-house and third-party legal teams), separate codes were produced, reflecting their intention. In the next step, R2 coded three, R3 coded two, and R1 coded all five subsequent interviews. New emerging codes and categories were discussed by all the researchers involved in this work in a further meeting. Finally, R1, R2, and R3 used the refined codebook to code the rest of the interviews, with R3 coding 8, R2 coding 22, and R1 coding all 30 interviews.

While the codebook was used to ensure consistency between coders coding different subsets, we note that *"even if coders agree on codes, they may interpret the meaning of those codes differently"* [50]. Since codes are considered an interim product in grounded theory, we valued the differences in code interpretation and thus refrained from using inter-rater reliability coefficients as a measurement instrument. However, through our codebook's iterative and highly collaborative construction, we ensured that the coders agreed in their understanding of how to use the category system [50]. We observed theoretical saturation between the 23th and 25th interview, i.e., no new properties emerged in interviews 25–30, and, hence, we stopped recruiting.

3.4 Ethical Considerations

The institutional review board (IRB) of our university approved our project. Participants were provided with a consent form outlining the scope of the study, the data use, participation risks, and retention policies. We also complied with the GDPR. Participants were informed that they could withdraw their data during or after the study without any consequences, as well as the practices used to process and store their data. We assured participants that we would only evaluate and publish de-identified data and quotes. All video and voice recordings were deleted after transcription. Participants had to give their consent before completing the demographic questionnaire and were additionally asked for consent and any additional questions before the interviews. They were also asked to download the consent form for their use.

3.5 Limitations

This section describes the limitations of our study, which have to be considered when interpreting the results.

We recruited participants on the freelance platform Upwork. This sample is certainly not representative of all developers and might not even be representative of other freelancer hiring services. Our profile analysis of potential participants for work experience in large companies was based on self-reported information and may suffer from several biases, including over- and under-reporting, sample bias, and social desirability bias. To mitigate social desirability bias, we specifically highlighted to participants that we are only interested in information about their communication processes and not judging their privacy knowledge, approaches, or processes in any way. While all participants were experienced in privacy processes at companies, some were only involved in projects as external councils or freelance developers for projects with limited time constraints.

Since grounded theory and theoretical sampling are not aimed at creating a representative sample, therefore, the results must be interpreted carefully concerning generalizability. Since we were interested in the communication of privacy requirements between developers and privacy experts, we mentioned privacy in our study description on Upwork. Thus, the software developers who participated in our study might be more privacy aware than the average developer. We observed a high rate of invited developers declining our job proposal on Upwork (15 of 31, 10 unanswered). A similar behavior was observed when recruiting team coordinators (6 out of 11, 3 unanswered). By contrast, this rate was very low for the privacy experts (2 of 12, 1 unanswered), indicating this target group might be more interested in working on privacy-related projects.

4 RESULTS

In the following, we present the main findings from the 30 interviews with developers, team coordinators, and privacy experts. We report results based on the categories of our codebook. We focus mainly on the perceptions of privacy requirements between the three groups, their communication, and how privacy requirements and the privacy process are handled within a company context.

4.1 Participants' Perceptions of Privacy Requirements (RQ1)

We asked participants from all three groups about their understanding of privacy, privacy concepts (e.g., PbD, PIA, FIP, and DM), and internal or external privacy regulations their company follows. Interestingly, we observed some participants focusing on security when asked about privacy.

4.1.1 Privacy Definition. All privacy expert participants provided clear definitions of privacy. For example, E10 gave the following explanation:

> *"Security is something that matters more with the infrastructure. So we have to put in place security measures in general, like cryptography, or secure our server somewhere [...]. And privacy is a bigger theme where also there is a part of security because data should be secured. But there is also much more. For example, the interest request or in general have a process in your company for being compliant."* (E10)

Team coordinator participants had a basic understanding of privacy and privacy regulation. Sometimes they had difficulties differentiating privacy and security issues (see Section 4.1.5). Seven developer participants lacked profound knowledge of privacy regulations or concepts but were responsible for fulfilling the privacy requirements (e.g., D1, D2, D4, D9, D10).

4.1.2 Privacy Concepts. Nine privacy experts were familiar with all the concepts of PbD, PIA, FIP, and DM (e.g., E1, E2, E3, E7, E10). They reported to have used many privacy concepts in their previous work (e.g., E2, E3, E4, E7, E10).

When asked about privacy concepts, eight team coordinator participants could not recognize all of them by name (e.g., C2, C3, C5, C7, C8). Three of them, however, reported to have implemented or used measures at their company without recognizing them by name (C1, C2, C7). Three others were unfamiliar with these concepts (C3, C8, C10). Five participants referred to consent, honoring people's preferences and control over data (C4, C6, C7, C8, C10). Further, four mentioned processes regarding data usage and storage (C5, C6, C9, C10). Three team coordinator participants specifically noted compliance with regulations such as purpose limitation or data collected on EU citizens has to be stored within the EU (C5, C7, C10). For example, C7 mentioned issues with data storage in the EU:

> *"So whatever kind of system do we buy or do we want to implement [...], the company has to be in the EU. The data is not allowed to leave European Union. It doesn't matter what kind of project it's about. I have got personally a lot of problems with that because you're really bound by that and it's really, really hard because EU does not have everything that, for example, [...] the American companies offer."* (C7)

By contrast, five developer participants could not recognize privacy concepts by name but reported to have used them before (D1, D2, D5, D6, D7). Three others, however, were unaware of most concepts (D4, D9, D10).

4.1.3 Company Internal Guidelines. All Privacy expert participants explained that companies often had internal guidelines concerning privacy. Six were responsible for creating the corresponding guidelines and privacy policies, which aimed to assist the development teams through the process of implementing privacy requirements (e.g., E4, E4, E5, E7, E10).

Six team coordinator participants mentioned templates, privacy policies, documentation, and questionnaires guiding them through the privacy process (e.g., C3, C6, C7, C9, C10). For example, C5 described the guidelines as follows:

> *"So based on different requirements of these applications and the landscape, we have a set of questionnaires and set guidelines there. And they have to answer that, or the questions, they have to justify that in the questionnaire to what they think and what they want us to take into consideration while we develop this project, while you build or run this project."* (C5)

Three participants (C4, C6, C7) faced issues with the company's internal guidelines, such as the fact that they were written in legal language and often were *"nebulous or ambiguous"* (C4). Participant C7 described their issues as follows:

> *"So very often I have to talk to them personally one on one or something like that, where they have to explain the question in a normal language. And then very often those, I mean, you can have a legal question which is being written in maybe ten words, and then those ten words [that] is one question, is very often broken down into five or six simpler questions where you have then now five or six questions which you have to answer. [...] I mean, it's not about language; it's not about, say, syntax, understanding of the question. It's more about contextual understanding."* (C7)

Seven developer participants mentioned internal documents being available within the company, helping them during the implementation of requirements. They used internal privacy policies, non-disclosure agreements, and documentation as guidelines (e.g., D4, D5, D7, D9, D10).

4.1.4 External Guidelines. All privacy expert participants mentioned different legal regulations being considered in the companies they were working for, depending on the area the companies were geographically located and operating. Commonly mentioned were GDPR and CCPA if the companies were operating in Europe or the United States. Participants also mentioned different regulations of local legislation. For example, a number of different legislations were mentioned by E9:

> *"[...] if it's the UK, then it's the Data Protection Act. [...] If it's the EU, then it's the GDPR, in the States it depends on which state you are from. So it can be anywhere from the California Privacy Act to the Digital Millennium Act, [...] Singapore as well, it will be in accordance with the PDPA, in South Africa, POPI."* (E9)

They were well informed about the laws companies have to follow depending on their service. While some were related to privacy, for example, the Health Insurance Portability and Accountability Act (HIPAA) [29] (E5, E6, E7), participants also mentioned regulations without a privacy focus. For example, E6 referred to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) [25] or the European Non-GMO Industry Association (ENGA) [10]. E7 mentioned special legislation concerning financial regulations, indicating that legal experts are often consulted beyond privacy laws.

Eight team coordinator participants could name regulations applying to their company context, for example, GDPR (e.g., C3, C4, C7, C8, C9), CCPA (C6, C7, C8, C9, C10), or other local regulations (C6, C8). Additionally, three reported to reference different privacy-related resources from the International Organization for Standardization (ISO) [30] (C4, C6, C9).

All but one developer participant referenced external guidelines being used within their work context. D5 mentioned retrieving information from the Open Web Application Security Project (OWASP) [67]. Four mentioned facing similar issues as the team coordinators concerning the understanding of guidelines and documents containing privacy advice by citing difficulties with legal language and missing definite descriptions or examples for their tasks (D1, D6, D9 D10). Five explicitly mentioned GDPR (D1, D2, D3, D4, D9) and four mentioned regional laws (D1, D2, D4, D8).

4.1.5 Security Focus. Privacy experts drew a clear distinction between security and privacy. Only E6 additionally referred to the term security when asked for privacy requirements.

By contrast, team coordinator participants often focused on security issues when asked about data privacy. Eight discussed encryption and authentication as part of privacy concepts and were concerned about potential attacks (e.g., C1, C2, C7, C8, C9). Still, five (C5, C7, C8, C9, C10) mentioned they saw a connection between the two topics:

> *"Yes, as a point of the privacy [...] is ensuring the data are appropriately encrypted. We also want to ensure that we look into the minute aspects and understand the criticality of the data, and we [...] define a process where we ensure those details are not leaked out, and it's appropriately secured."* (C5)

Further, seven team coordinator participants referred to employees with security-related roles within the company as being also responsible for privacy (e.g., C4, C6, C7, C8, C10), indicating that security and privacy are often handled as one issue in practice.

While eight software developer participants referred to privacy-related topics such as consent, storage of sensitive information, and authorized access (e.g., D3, D7, D8, D9, D10), five developers also referred to security concepts (D2, D6, D7, D8, D9). For example, encryption was mentioned as a common concept - arguing that if user data is encrypted, it is secure against attackers: *"The biggest guarantee clients, companies, and agencies can be given is some form* *of encryption [...]. However, no human without [...] knowledge of an encryption code has access to that data"* (D2). Additionally, concepts like authentication, zero-knowledge proofs, and penetration testing were mentioned by four software developer participants (D3, D6, D8, D9). Thus, developers tended to think about security when asked about privacy as they seemed more familiar with implementing security measurements and preferred to be given specific security requirements instead of privacy guidance. While the mentioned security issues are important and contribute to the security of user data, they do not address the fair use of collected data according to laws and regulations, indicating that the focus often lies on attack scenarios instead of unintentional misuse by the data collectors themselves. Participants D8 and D9 identified security as necessary to achieve privacy. However, five agreed that considering only security is insufficient (D5, D6, D7, D8, D9).

4.2 Communication of Privacy Requirements (RQ2)

In the following, we describe involved parties in the communication process of privacy requirements, exchanged information, good practices, participants' wishes for improvement, and communication challenges.

4.2.1 Involved Parties. When asked about privacy experts, 21 participants referred to in-house lawyers and DPOs (e.g., D5, D9, C3, C7, E4). Some larger companies have a department specialist privacy team, while smaller companies generally rely on third-party consultants, as mentioned by six participants (e.g., D7, C6, C8, E1, E5). Participants D9 and C9 mentioned contacting government entities to communicate on privacy. Privacy experts are tasked with collecting information about the project, referring to internal or external data regulations, and creating privacy requirements, which are often sent to developers in indirect communication according to 14 participants (e.g., D7, C2, C5, E1, E4).

Nineteen privacy expert participants and developer participants explained they were often not directly contacting each other but via employees with leadership positions (e.g., D4, D8, E1, E2, E9). The role and background of these intermediaries can vary - team or product leads, product management, or product owner - often depending on company size. In smaller companies, the intermediary role is performed by a member of the leadership team or the company owner. Companies developing software at clients' request often included the clients in the communication on privacy and thus relied on them to provide the requirements as described by 11 participants (e.g., D3, D8, C6, C8, E4). Additionally, departments like sales, marketing, and human resources were also mentioned as being involved. All team coordinators we interviewed received privacy requirements from privacy experts and forwarded them to the software developers. Thus, they could take the role of a man in the middle. They had background knowledge of software development rather than privacy data regulations.

Nine participants from all groups (e.g., D2, D8, C4, E7, E10) mentioned experienced colleagues who were aware of privacy issues and could take responsibility for privacy within the development team. Past research referred to these individuals as privacy champions [82], raising awareness for privacy issues and being available for privacy-related questions during the implementation process:

> *"So I think one of them [development team] comes from a privacy background, from a large, kind of data company in the US. And so I think that experience helps a lot because [...] within the engineering squad, they go to that particular individual."* (C4)

Further, employees whose job description indicated a focus on security were reported by nine participants to be active in privacy communication (e.g., D5, D8, C1, C6, E6).

4.2.2 Starting Point. Participants were asked about their experience with starting points in projects addressing privacy requirements. Nine privacy expert participants mentioned they usually are involved from the beginning of a project (e.g., E1, E4, E5, E8, E9), five noted being involved in a project upon request (E1, E2, E4, E7, E8), and four described occasions where they became involved after the product was already deployed (E1, E4, E5, E6).

Five team coordinator participants mentioned starting the privacy process at the beginning of a project (C3, C4, C5, C7, C8). Five mentioned sprints or testing phases (C2, C4, C5, C6, C9). Lastly, C6 described that sometimes privacy was considered only after deployment.

While six software developer participants mentioned that the privacy process starts from the beginning (e.g., D1, D2, D3, D4, D9), three (D5, D7, D9) said the testing phase was their usual starting point.

4.2.3 Challenges. Six privacy expert participants (e.g., E1, E2, E5, E6, E8) mentioned that software developers often perceived them as a disruptive factor in software development: *"You're always seen as the blocker"* (E2); *"I'm the enemy or I'm the one who says, No, you [CEO] can't do that"* (E1). However, six privacy expert participants acknowledged that it is challenging for software developers to understand legal text, thus further affecting the communication between these two groups of individuals (e.g., E1, E3, E5, E8, E9). Missing information from the communication partners affected the privacy experts' ability to successfully accomplish tasks, such as providing privacy requirements to the development teams, was mentioned by five privacy expert participants (E4, E5, E7, E8, E9).

Team coordinator participants mentioned different challenges concerning privacy requirement communication. The overview of the high amount of different data regulations was mentioned to be specifically challenging: *"because there are so many regulations"* (C7); *"And it is very long. Very tiring to read this APP [Australian Privacy Principles]"* (C6).

The most common issue developer participants mentioned was that privacy was not treated with priority by the companies, which was mentioned by six developer participants (e.g., D1, D2, D4, D5, D9).

> *"Even in the larger organizations, I've never seen anyone actually do a proper formal assessment after it's been built, and it's working to see whether it meets the privacy requirements that were given earlier in the process. And the smaller clients, they didn't think of it. [...] They don't actually want to go and check whether they're, they're doing it properly, or whether I've done it properly, I suppose, really in that case."* (D1)

Four developer participants felt they were rarely involved in the communication process of privacy requirements (D1, D6, D7, D8) and requested someone they could contact concerning privacy requirements:

> *"[...] the person to give you the information may be very busy and they just point you to a file [...] or they just give you the entire file and you have all of the clients' information in front of you, which you are not supposed perhaps to access."* (D7)

Additionally, three (D1, D9, D10) complained that the legal requirements were hard to understand for them *"the HIPAA [...] those things are written by lawyers, and programmers are reading that"* (D9). By contrast, privacy experts were perceived as disruptive and lacking the technical expertise by two (D6, D9) developer participants *"He's [privacy expert] not technical like he doesn't have the software knowledge"* (D6).

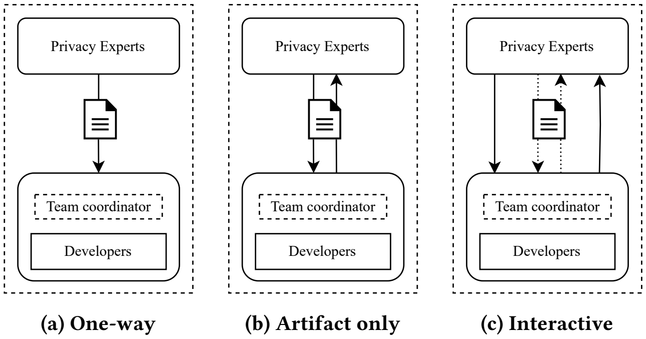
4.2.4 Good Practices. Seven privacy expert participants noted that having a clear process and open communication would be helpful for a good working relationship with the development team (e.g., E2, E6, E8, E9, E10). One key factor mentioned for good practice was involving privacy experts early in the software development process:

> *"I think it's more of where we [privacy experts] are on the planning stage, and we have provided you [project manager] with a requirement. So it's just up to them [software developers] to implement what we have recommended."* (E8)

Two also mentioned that good documentation of the communication process could help clarify the requirements (E7, E9). Additionally, three others wished for a *"common language"* (E2) and more understanding of legal requirements from developers (E1, E2, E8).

Six team coordinator participants perceived that open communication with the involved parties and having a flat hierarchy could increase the quality of privacy requirement communication (e.g., C1, C3, C7, C8, C10), e.g., by also involving software developers: *"we [team coordinators] prefer to have the software developer on call with the privacy experts"* (C8). One also mentioned colleagues with whom they work closely as ample support: *"Luckily, in my case, I have a few colleagues [...] who have worked very close to data privacy. And so I can kind of, I guess, collaborate with them"* (C4). C2, C4, and C10 wished for more direct, proactive, and improved communication with privacy experts. Providing software developers more context might also improve the development process: *"I think they [software developer] can always get more context around the problem"* (C4). Besides, C5 mentioned that better communication tools (e.g., Issue Tracker Software) could also improve the communication process with software developers.

Four developer participants mentioned that discussing privacy issues openly with the involved parties positively influences their company and is helpful concerning the developers' challenges, such as missing information and the lack of communication (D1, D6, D7, D8). Additionally, six (e.g., D2, D5, D8, D9, D10) stated that the communication was perceived helpful when legal requirements were clarified *"He [lawyer] will explain things in great detail and make sure the developer understands them correctly"* (D9). Four developer participants felt that being part of the discussion, especially at the beginning of the software development process, might improve the communication of privacy requirements (D1, D3, D7, D8). This could be achieved by, e.g., *"coming up with a communication department"* (D8). Additionally, D2 and D6 noted that having clear protocols would support communication between all parties. In many cases, they were unsure how to reach out for clarifications.



(a) One-way **(b) Artifact only** **(c) Interactive**

Figure 1: Communication pattern between privacy experts and development teams.

4.2.5 Communication patterns. We identified three main patterns participants described in the communication process concerning privacy as shown in Figure 1. While companies would not always stay strictly to one pattern and might employ solutions mixing elements from the patterns, the three patterns present the main ways of communication between the groups.

The first pattern (Figure 1a) was most common and described as a "one-way communication" if external privacy experts created the requirements, as they were often hired only to create the requirements and unavailable for questions. In these cases, software development teams only received the requirements and had to resolve potential questions themselves. In a second pattern, "artifact only" (Figure 1b), the communication between the privacy experts and the software development teams happened on the documents containing the privacy requirements. Software developers would leave comments or create issues if they required clarification, had questions, or found issues, to which the privacy experts would reply. Lastly, some participants described the process as very interactive (Figure 1c): software development teams and privacy experts would directly communicate with each other and discuss software projects and requirements aimed to be fulfilled by them. This would mean directly involving the employees from both sides in meetings and contacting each other with questions. Further, both sides could leave comments and discuss issues in the privacy artifact.

4.3 Creation and Implementation of Privacy Requirements (RQ3)

In the following, we describe the creation, implementation, and verification process of privacy requirements.

4.3.1 Exchanged Information. To create privacy requirements for their projects, privacy expert participants reported requiring access to project information. Eight privacy expert participants mentioned they were given a product description covering the system's purpose, functionality, and technical requirements (e.g., E1, E2, E4, E8, E9). All but one privacy expert participant stated that they need to know about the collection of customer data (e.g., E1, E4, E5, E7, E10) or the storage of that data (e.g., E1, E2, E3, E6, E9). Additionally, seven privacy expert participants mentioned they need to know the 3rd parties involved in the delivery of a service or what security measures and policies are already in place (e.g., E1, E4, E5, E6, E9). This information is often collected from software development teams via questionnaires asking about sensitive information collected in different projects, as described by three participants (E1, E4, E6). The privacy experts evaluate the questionnaires and return them to the developers, with critical issues marked for the development teams to take care of. E7 and E8 mentioned OneTrust [56] as a tool to communicate the questionnaires for the PIA to the companies. Additionally, seven privacy expert participants reported performing risk assessments of the applications (e.g., E2, E4, E6, E7, E8).

4.3.2 Implementation. When privacy expert participants were shown examples of data collection for advertisements, six stated the requirements represented what they would encounter as part of their work (e.g., E2, E3, E4, E6, E9). Four other participants noted that they are unlikely to work on such privacy requirements as their company is not involved in advertising (E1, E7, E8, E10). All privacy expert participants perceived the more technical requirements concerning microphone usage as realistic. However, two mentioned it would probably require a particular data collection form as they were unaware of a practical application at their workplace (E4, E8). Six privacy expert participants said they often send messages to the development teams and ask them to stop collecting sensitive data (e.g., E2, E3, E6, E8, E10).

Three team coordinator participants mentioned they would expect privacy requirements to be more similar to functional requirements (C1, C3, C7). A key example concerned how "access control" was defined, leaving six unable to understand what was required to be implemented (e.g., C2, C4, C5, C6, C8).

> *"So I think in this example, like understanding [...] who are the users who get this access or who within the organization, what access type, what are the roles and responsibilities of that access? And then is it the whole table? Is it parts of the table?"* (C4)

Further, as described by C6, even seemingly simple requirements like implementing a maximum retention period might not be as straightforward as they seem:

> *"So for example, that form is something that I deleted. But it's there in our backup and that form can be brought back into life after we restore our backup. So having that mechanism, checking that mechanism is important there."* (C6)

Three team coordinator participants would regularly remind their developer teams of the requirement to make sure audio data was not collected, (C7, C8, C10), with C7 reporting that they would further specify the requirements into tasks for the developers. However, five mentioned the example did not apply to their work context (C1, C2, C6, C7, C10), as they were not involved in collecting data.

Eight developer participants reported to be able to handle the two more technical requirements (e.g., D1, D2, D6, D7, D10). Like the team coordinator participants, seven developers perceived *"access control"* needing to be clearly defined (e.g., D3, D4, D6, D7, D8). *"The first thing I would do would probably be to ask [...] what the access control should be, so what the requirements are for the access control, who what type of user can access what in that table?"* (D6) Nine participants were generally able to describe technical details on the implementation of the requirements, for example, developing an automated script to take care of data deletion in case the retention period was over (e.g., D1, D2, D5, D7, D10). However, seven developers mentioned that the third requirement concerning advertising would not be a requirement they expect to encounter, as they had no control over advertising (e.g., D2, D4, D5, D6, D9).

4.3.3 Verification. When asked about the verification process for the correct implementation of privacy requirements, eight experts would rely on the information given by other employees (e.g., E1, E5, E7, E8, E10). Five (E1, E4, E7, E8, E10) specifically mentioned they had to rely on other employees for verification since they lacked the technical skills to check the implementation:

> *"If we speak about, you know, source code or going through the development that I would not be able to check it on my own because I do not have the technical background or knowledge. So I would of course ask for the responsibility of the persons involved."* (E1)

Further, E6 perceived his responsibility only in consulting. While four privacy experts reported that privacy issues might be rechecked during regular audits (E2, E3, E7, E8), five participants noted the lack of a verification process for privacy requirement implementation (E1, E4, E5, E6, E9). *"It's normally just sent out and then that's it"* (E9). Responsibility for the proper implementation of privacy requirements was shifted to software developers by five privacy expert participants (E1, E4, E5, E7, E8).

For our examples, four team coordinator participants often mentioned testing the privacy implementation themselves (C6, C7, C8, C9). In three cases, they reported creating dummy accounts with different access levels to check if access control was correctly implemented into a table (C6, C8, C9). Another potential form of verification mentioned was to check the implementation through code reviews, which were mentioned by three team coordinator participants (C7, C8, C9).

As already observed for team coordinators, two developer participants mentioned creating test cases themselves to verify privacy requirement implementation (D2, D8). For example, D8 would create accounts with different access levels and verify that the access control was implemented correctly. Similarly, code reviews were mentioned as a means of verification by two developer participants (D6, D10).

4.3.4 Challenges. Five privacy expert participants perceived that software developers often don't understand the privacy requirements (E1, E2, E3, E5, E9) they create for them and/or are unwilling to implement them: *"It happened to me that I had a bit more difficult exchanges in terms of negotiation because simply they did not want to implement certain issues just because it didn't make sense for them"* (E1). Three privacy expert participants also mentioned a lack of teamwork and clear responsibilities on privacy issues (E4, E6, E7), which hinders the privacy process.

> *"Some developers don't care about privacy, so the developers don't care about security. Some security people don't care about developing. [...] So people just don't want to learn a new task, or they would be like, it's not my job. I don't want to do it. Give that to a security person."* (E6)

Four team coordinator participants reported issues with the quality of the in-house privacy guidelines or guidelines provided by experts. They often had to ask for clarification of tasks and for detailed instructions on how to fulfill a particular requirement (C4, C6, C7, C8). C7 described issues that arose when they were required to give external users access to internal documents:

> *"One requirement from two weeks ago [...] was, we have to enable downloading invoices to our customer. Those invoices contain data of our employees, what they have been working on for the customer. [...] So that's something that you cannot disable the access [...] from third parties outside of the company's network to this data. Now, it is about where is this data located? Because the requirement is often just like that. It is not a requirement. It's very often just a wish. [...] So some kind of data is stored in the archive, the other data in the ERP system and the third data is in Excel files and we have to gather all that data and then create a PDF document about it and then allow the document to be downloaded. [...] That is still in communication with the privacy officer because we cannot say with 100% certainty that that data is going to be always secure."* (C7)

Four team coordinators mentioned that high-complexity systems would make it very difficult to implement the requirements accurately, as changes to the system could influence many parts (C3, C6, C7, C10). Additionally, C7 mentioned that regular testing and code reviews help spot potential errors. C4 noted having an experienced person on the team would help during the implementation.

Five software developer participants complained about privacy requirements not being set into context and missing clear tasks or instructions applicable to the implementation phase (D2, D3, D6, D8, D9) *"[...] I think most of the privacy guidelines I've seen are relatively ambiguous. You know, it's left on how you choose to interpret it"* (D2). Vague guidelines were blamed for causing issues during implementation by two participants, as it was often unclear what was required from the developer (D9, D6).

> *"So there are a lot of scenarios that are not directly covered inside the explaining regulation, and that's where the back and forth with the regulating body comes because you need to give them examples. What if this, what if that, will that be compliant to you?"* (D9)

Still, four developer participants (D1, D2, D3, D9) mentioned providing examples as a positive factor: *"And the people who were the first ones to implement GDPR, those are the ones who struggled, but the ones who come after them, it's much easier for them because they have examples"* (D9).

Three developer participants complained that complex systems would make it very difficult to implement the requirements accurately (D2, D7, D8), as many parts of the system would have to be reworked: *"So it means, and it depends on so many other components. So you have to go back and start redesigning or refactoring of the system code that you've done"* (D7). Additionally, D2 mentioned having an experienced person on the team would help during the implementation.

4.3.5 Tools. Two team coordinators said using Amazon Web Services [8] (C6, C10) is a positive factor for implementing privacy. They noted many privacy-related issues were already taken care of by this service. However, C5 complained about needing better tools to implement privacy requirements easily.

Two developer participants referred to third-party tools with privacy features already in place. For example, they mentioned Microsoft Azure [53] (D9) or Google Cloud Services [33] (D6), explaining the services already fulfill many requirements regarding privacy.

4.4 Employment Status

We explored if participants' backgrounds might influence their perceptions of privacy communication and found that their current employment status might be relevant. Freelance or part-time privacy experts indicated to have experienced issues with missing information, such as technical information or information on data retention, to be especially challenging for privacy requirement creation. Further, freelance or part-time team coordinator participants called for more open and frequent communication on privacy than full-time employed team coordinators. Freelance or part-time developers mentioned difficulties fulfilling requirements in complex applications as it was difficult for them to asses how changes would influence the remaining system. They also mentioned communication issues such as missing context and clear tasks more often than software developers employed full-time. These findings highlight the existence of communication problems within companies, as outsiders (e.g., self-employed legal experts being hired as consultants or freelance developers) struggle to receive the information required for their tasks.

4.5 Privacy Requirements in Companies

While our analysis focused on the communication and implementation process of privacy requirements between developers and privacy experts, we also discuss the company context as a key factor.

4.5.1 Motivation for privacy. Seven privacy experts had the objective for the company to be compliant with privacy regulations (e.g., E3, E4, E7, E9, E10) and two to pass potential audits by an external government entity (E2, E6). Eight mentioned the fear of fines (e.g., E1, E2, E5, E7, E9) and four named legal issues (E4, E6, E7, E9) as the primary motivators for ensuring the correct implementation of privacy requirements: *"Right now, it's just everyone hopping onto the bandwagon to show [...] compliance so that we don't get penalized for it because the penalties are quite high"* (E9). The objectives of team coordinators were compliance with legislation (C4, C6, C8, C9, C10) and fulfilling customers' wishes (C6, C7, C8). Two feared that bad privacy could tarnish their reputation and thus decrease their willingness to continue cooperating with the company (C1, C5): *"Obviously, there's a reputational risk that our company would face if we're not handling our client data as a good steward"* (C1). Similarly, while four developer participants' primary motivator for implementing privacy was also to comply with legislation (D2, D4, D7, D8), D3 explicitly mentioned the wishes of their customers as a motivating factor.

4.5.2 Company-related challenges. Seven participants across all three groups reported that companies often were restricted by the lack of project resources (e.g., D3, C2, C5, E2, E4). This could include funding tools, having dedicated employees focusing on privacy issues, or hiring experts to advise the company, as well as the time they can set aside for privacy issues. *"The budget is quite limited, and for them [company], it is, let's put it this way, quite expensive to have extensive discussions with the privacy professionals"* (E4). In addition, the difficulties increased for globally-operating companies, as there might be multiple different pieces of legislation that can apply.

> *"At [company], my role is the America's privacy officer, so I'm primarily in charge of U.S., Canada, Latin America. Right. And many of those countries now have privacy laws as well. Mexico, Brazil, Argentina."* (E7)

Further, the involvement of third parties or other departments can cause the company to rely on the privacy implementation of others without being able to verify that correct procedures are indeed in place to secure the collected information: *"[...] as soon as you give the keys to this third party, to some degree, all bets might be off, right?"* (E7)

4.5.3 *Privacy training.* Eight participants from all three groups asked for awareness (e.g., D1, C3, C4, E3, E5), nine more experienced employees (e.g., D2, D8, C8, E1, E8), and seven for training (e.g., D2, C2, C4, E6, E8) within the company:

> *"[...] the best way for any anyone in a tech company is to make sure that they are compliant with data privacy requirements is to really do the training to emphasize with them and provide them with the context. So they really need to understand why [...] are we implementing this?"* (E8)

This could also positively influence the company culture, which was wished for by E7, C6, and C7.

5 DISCUSSION AND RECOMMENDATIONS

In this section, we discuss our findings deducted from the results of our interviews. Considering our codes, memos, categories, and the experience with participants, we constructed an explanatory theory grounded in the data collected:

> **An existent communication gap between privacy experts and software developers hinders the implementation of privacy requirements. Privacy experts often do not have an understanding of the software development process and developers' tasks. By contrast, developers do not possess knowledge of privacy laws, regulations, and voluntary codes of conduct. Privacy experts pass privacy requirements to developers, who struggle to infer from them what controls where to implement and how to verify whether the requirements have been met. Communication patterns varied from an interactive collaboration between experts and development teams to one-sided communication, where requirements were handed over in a one-time manner while shifting responsibility and interpretation to the development team.**

Figure 2 summarizes the obstacles supporting our theory and guidance on combating them in promoting a common ground.

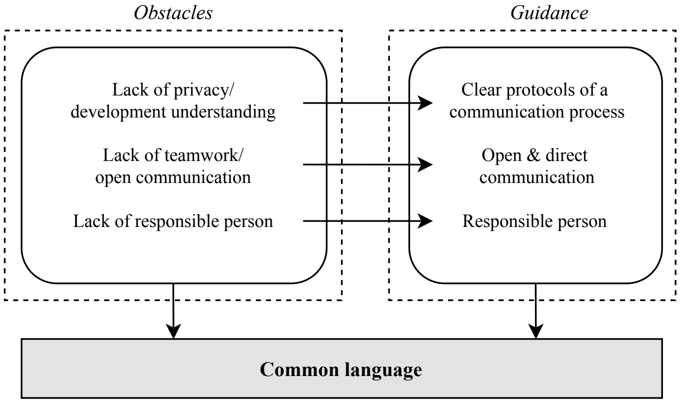

Obstacles
Guidance
Lack of privacy/ development understanding
Lack of teamwork/ open communication
Lack of responsible person
Clear protocols of a communication process
Open & direct communication
Responsible person
Common language

Figure 2: Obstacles and guidance to a Common Ground between privacy experts and software developers.

Common Ground Theory. Concepts from the field of psychology might offer insights into why this communication gap exists. For example, the Common Ground Theory [20, 22] recognizes the need for communication parties from different perspectives and fields to understand each other. To communicate effectively, the parties involved in the communication process need to establish a Common Ground containing "the sum of their mutual, common, or joint knowledge, beliefs, and suppositions" [20, p. 93]. This frame is mainly based on two sources: the *Communal Common Ground*, which is created through stereotypical assumptions based on attributes of the communication partner (e.g., age, gender, or profession), and the *Personal Common Ground*, which is built upon direct experiences with the communication partner. During the communication process of legal requirements in the software development process, two different parties are communicating with each other: legal experts, who are laypersons in the field of software development, and software developers, who are, in turn, laypersons in the area of privacy law, but experts in the field of software development. To effectively communicate, experts need to anticipate and adapt the laypersons' perspective [15, 16]. The Communal Common Ground might not be accurately established because experts can have different cognitive representations and knowledge systems about their fields compared to laypersons [15]. Since we explored the communication between software development experts and privacy experts, these issues could disrupt communication in both directions. Further, the limited interaction of the two groups (see Section 4.2.5) could hinder the creation of a Personal Common Ground. The parties involved could switch to more direct forms of communication (e.g., face-to-face) [21] and establish privacy requirements and protocols in collaboration, ensuring that both parties address any unclear points. Establishing a common vocabulary and understanding of the risks might be essential for this.

Expertise of privacy experts and developers. Communication between software developers and privacy experts was perceived as complex due to the lack of knowledge of each other's fields of work. A potential cause for this could be an inaccurate representation of the Communal Common Ground, as outlined earlier. Often software developers had no legal background, and thus their understanding of requirements was hindered, e.g., by legal language (see Section 4.1.3). Therefore, software developers tended to confuse data privacy and security. They perceived privacy requirements as hard to understand due to the lack of context, unclear instructions, missing examples, and a language barrier. Further, they wished to be actively involved in the communication process and asked for a responsible party to contact when dealing with unclear privacy requirements. By contrast, privacy experts without software development experience faced difficulties understanding the software development process and technical details, making it hard for them to create privacy requirements to be used by software developers. Some privacy experts mentioned product artifacts or risk assessments as one of their main sources for creating requirements (see Section 4.3.1). Depending on how well or poorly the artifacts are described (e.g., documentation, test cases, or architecture), interaction with the development teams is highly relevant. During the walkthroughs, some privacy experts perceived measures taken to fulfill the requirements as "too technical" (see Section 4.3.3) to be able to verify the implementation.

Mutual perception. Privacy experts complained about software developers who were not motivated to comply with privacy requirements because they did not understand or care about privacy (see Section 4.3.4). They often felt to be considered a deterrent or the *"enemy"* by developers since they were viewed as responsible for blocking the development process. This obstacle could make it challenging to establish a Personal Common Ground, consequently affecting future communication. However, privacy experts also wished for a clear communication process and direct communication with software developers instead of referring them to privacy requirements. By contrast, developers mentioned that they struggled to understand privacy requirements and considered them ambiguous and not detailed enough (see Section 4.3.4). Perception also depended on how the organizational structure and communication process were designed. Often team coordinators (e.g., product owners or technical team leads) were the pivot point for transforming higher-level requirements into technical requirements and breaking them down into work packages. But even if the communication between the privacy experts and a team coordinator is bridged, technical decisions still need to be made on handling the privacy requirement. Consequently, the development team needed to be involved.

With this, we argue that the development teams' perception is strongly influenced by the fact that (i) the technical detail of the requirements is often insufficient from the teams' point of view and (ii) privacy requirements do often lack a "visible" value. Developer participants complained that the privacy requirements they received did not specify how to be achieved, so they had to figure out their implementation by themselves. Thus, requirements should specify why they are relevant in the context, concrete steps that need to be taken by the development teams and the desired outcome. As privacy experts may lack the technical knowledge to create requirements that are detailed enough to cover edge cases present in the system, development teams need to be able to contact the experts with questions and requests for clarifications to ensure correct implementation.

5.1 Recommendations for Industry

Our privacy expert participants did not have expertise in verifying privacy requirements on a technical level. Checking the source code is rather a rare procedure. Similar to processes adapted in the security field, such as regular penetration tests [100], privacy should be part of all stages in the software development process. However, performing penetration tests is not enough for a sustainable change towards more security within the product teams [65]. Therefore, promising tools were introduced in the security field that can be integrated within the software development build pipeline (e.g., static analysis, dependency checking) [27, 66, 77, 90]. It seems the privacy field is still lacking the usage of similar tools within the company context. While the OWASP community aims to make security accessible and understandable for everyone, our developer or team coordinator participants did not refer to a similar guide concerning privacy. Similar privacy-focused best practices accessible to software developers might further improve privacy implementation.

Educate development teams early about privacy concepts. We encourage businesses to educate their development teams on privacy concepts, which is crucial to ensure an early adoption in the development process. This may further help to establish a more accurate Communal Common Ground, making communication easier. Implementing privacy requirements late in the development process due to companies' constraints such as limited project resources (see Section 4.5) will most likely incur higher cost. Thus, allocating the resources to educating development teams about privacy concepts early in the development process is very likely more efficient. For example, adopting concepts like data minimization reduces effort if implemented early in the development process. Fixing a product late in the software development cycle may require substantial re-writing and redesigning to ensure the product will still function correctly with fewer data. Thus, development time and funding can be saved by taking care of issues early. However, developers need to be supported during this step, as they may feel restricted by the requirements (see Section 4.2.3). Within our study, developers were accountable for verifying implemented privacy requirements. However, as most were confused about privacy and security and did not know common privacy concepts, we highly recommend establishing a baseline of knowledge for the development teams by going beyond presenting them with privacy requirements on a one-way communication line. Teaching privacy concepts to software developers might have multiple advantages for companies, as it may help the development teams to (i) fulfill requirement concepts from different domains (e.g., through data minimization), (ii) gain awareness of privacy and privacy risks, and (iii) might close the communication and language gap between privacy experts and the development team.

Build a privacy-supporting company environment. Our study showed that developers consider privacy experts as disruptive fostering an adversarial relationship between software engineers and privacy experts, resulting in a negative privacy attitude. Thus, it makes it less likely that developers will actively approach privacy experts or pay more attention to identified privacy issues. Consequently, bad habits and routines might be established, which are resource-intensive to correct, as already learned from numerous attempts to change behavior in the security domain [38, 42, 65, 91, 99]. Limited interaction will further obstruct the creation of Personal Common Ground between the two groups, making communication more difficult. We call for the support of privacy experts, as technical expertise cannot always be expected. Technical experts are required to explain the system, as well as verification of the implemented privacy requirements. Consulting privacy experts in one direction (artifacts only) will not ensure the correct implementation of privacy requirements.

5.2 Recommendations for Academia

This study is the first step in offering insights into a highly complex communication problem. Based on the resulting theory, we suggest the following research objectives for future work:

Verification of privacy requirements. Verification of privacy requirement implementation is often missing and threatens users' privacy. More research is required on how the verification process could be improved for developers on the technical side and privacy experts on the legislation side.

Privacy champion. While security champions were explored in research [35, 37, 91], it is unclear yet who is considered taking responsibility and acting as a privacy champion [82], developers, team coordinators, or privacy experts? Team coordinators were often tasked with the fulfillment of privacy requirements. Having employees with experience or certifications regarding privacy in leadership positions might be a good way to embed privacy principles. These employees could have the role of supporting developers but also understand the reasoning and importance of the requirements provided by the privacy experts. Further, they could provide technical details to the privacy experts involved in creating guidelines and requirements.

Differentiating security and privacy. Many developers and team coordinators seemed to think of the same issues concerning privacy and security. Thus, participants often focused on possible scenarios with attackers but ignored the potential incorrect collection or misuse of personal data. Further research is needed on how developers can be supported with better-differentiating privacy and security issue implementation. One possible direction might be exploring privacy education in Computer Science (CS). Education can play a crucial role in implementing security and privacy requirements and should start early, e.g., in the university context. It might help to establish a more accurate *Communal Common Ground* by improving developers' understanding of privacy. Recommendations have been issued for the security education of computer science students [81, 83, 101], suggesting early education improves the students' security mindsets and mental models. Introducing software developers to privacy and legal concepts in the context of software development early in their studies might sensitize future software developers to potential privacy threats. With many CS curricula showing little focus on privacy, educating CS students on privacy-relevant topics might be a good starting point to sensitize future developers to privacy issues [88]. Future research should explore the role of privacy education. In particular, it would be interesting to learn where software developers gather their information when implementing privacy requirements and which sources they base their decisions on.

Developer-friendly privacy requirements. Participants often expressed issues translating requirements or expert feedback into clear tasks to fulfill certain privacy requirements. For creating privacy requirements, it might be necessary to consult not only privacy experts but also software developers tasked with fulfilling them. More research is needed in requirements describing the desired outcome and concrete implementation steps the development teams have to take. Further privacy requirement tasks might be explored in future work (e.g., right of access, right to erasure). Participants also mentioned that they faced issues processing data across international borders (e.g., processing EU citizens' data in the United States) and difficulties implementing data retention policies.

Fostering a healthy relationship between privacy experts and developers. Different parties with different backgrounds perceive each other in a blocking manner has also been found in security research (e.g., [9, 13, 35, 91]), such as end users seeing security experts and the measures they deploy within their company as a hindrance, resulting in a dysfunctional relationship between the two groups [51]. This may limit the interaction of the groups, hindering the establishment of a Personal Common Ground. With this work, we advocate against fostering an adversarial relationship between privacy experts and developers, as already observed in the security field [34]. To combat these issues, involving experts early in the software development process, as learned in the security field exploring the communication of staff and security experts [9], might be a good starting point for future privacy research.

6 CONCLUSION

Despite measures to improve user data protection (e.g., GDPR/CCPA), data breaches threaten user data worldwide on a daily basis. Understanding the creation, communication, and implementation process of privacy requirements is the first step to improving user data privacy sustainability. Compared to previous work acknowledging developers are struggling with privacy tasks, we focused on the privacy requirement implementation process within a company context concerning relevant roles involved.

In this study, we conducted 30 interviews with privacy experts, software developers, and team coordinators using a grounded theory approach. We analyzed the different understanding of privacy concepts and how team coordinators, software developers, and privacy experts perceived the communication. Additionally, we explored how privacy requirements were created, forwarded, and implemented. We contribute a theory grounded in our participants' data, suggesting a communication gap between software developers and privacy experts. Further, we highlight common obstacles in the communication between privacy experts and developers, discuss how to address them and provide recommendations on embedding privacy requirements into the software development process.

This study presents a first qualitative look at the communication gap of privacy requirements as a research problem. Future work should examine different types of developers. Additionally, to explore the generalizability of the findings, the sample size needs to be increased to gather quantitative data.

ACKNOWLEDGMENTS

We thank our anonymous reviewers and shepherd for helping us improve our paper. We further thank Luisa Jansen for her valuable feedback. This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

REFERENCES

[1] Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, Doowon Kim, Michelle L Mazurek, and Christian Stransky. 2017. Comparing the Usability of Cryptographic APIs. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 154–171.

[2] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. 2016. You Get Where You're Looking for: The Impact of Information Sources on Code Security. In *2016 IEEE Symposium on Security and Privacy (SP)*. 289–305. https://doi.org/10.1109/SP.2016.25

[3] Y. Acar, S. Fahl, and M. L. Mazurek. 2016. You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. In *2016 IEEE Cybersecurity Development (SecDev)*. IEEE Computer Society, Los Alamitos, CA, USA, 3–8. https://doi.org/10.1109/SecDev.2016.013

[4] Yasemin Acar, Christian Stransky, Dominik Wermke, Michelle L. Mazurek, and Sascha Fahl. 2017. Security Developer Studies with Github Users: Exploring a Convenience Sample. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 81–95.

[5] Abdulrahman Alhazmi and Nalin Asanka Gamagedara Arachchilage. 2020. Why are Developers Struggling to Put GDPR into Practice when Developing Privacy-Preserving Software Systems? (Aug. 2020).

[6] Abdulrahman Alhazmi and Nalin Asanka Gamagedara Arachchilage. 2021. I'm all Ears! Listening to Software Developers on Putting GDPR Principles into Software Development Practice. *Personal and Ubiquitous Computing* 25, 5 (2021), 879–892.

[7] Noura Alomar and Serge Egelman. 2022. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies* 4, 2022 (2022), 24.

[8] Amazon. 2023. Amazon Web Services. Retrieved Mar 13, 2023 from https://aws.amazon.com

[9] Debi Ashenden and Darren Lawrence. 2016. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Security & Privacy* 14, 3 (2016), 82–87.

[10] European Non-GMO Industry Association. 2023. European Non-GMO Industry Association. Retrieved Mar 13, 2023 from https://www.enga.org

[11] Oshrat Ayalon, Eran Toch, Irit Hadar, and Michael Birnhack. 2017. How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17 Companion)*. Association for Computing Machinery, New York, NY, USA, 135–138. https://doi.org/10.1145/3022198.3026326

[12] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, and Lorrie Cranor. 2014. The Privacy and Security Behaviors of Smartphone App Developers. (01 2014). https://doi.org/10.14722/usec.2014.23006

[13] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The Compliance Budget: Managing Security Behaviour in Organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (Lake Tahoe, California, USA) *(NSPW '08)*. Association for Computing Machinery, New York, NY, USA, 47–58. https://doi.org/10.1145/1595676.1595684

[14] Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. 2019. Engineering Privacy by Design: Are Engineers Ready to Live up to the Challenge? *The Information Society* 35, 3 (2019), 122–142. https://doi.org/10.1080/01972243.2019.1583296 arXiv:https://doi.org/10.1080/01972243.2019.1583296

[15] Rainer Bromme. 2000. Beyond One's Own Perspective: The Psychology of Cognitive Interdisciplinarity. *Practicing interdisciplinarity* (2000), 115–133.

[16] Rainer Bromme, Regina Jucks, and Anne Runde. 2005. Barriers and Biases in Computer-Mediated Expert-Layperson-Communication: An Overview and Insights into the Field of Medical Advice. *Barriers and Biases in Computer-Mediated Knowledge Communication: And how they may be overcome* (2005), 89–118.

[17] Cambridge. 2023. Cambridge. Retrieved Mar 13, 2023 from https://dictionary.cambridge.org/de/worterbuch/englisch/expert

[18] Kathy Charmaz. 2006. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis.* Sage. cited on p. 25, 96, 97.

[19] Kathy Charmaz. 2008. Constructionism and the Grounded Theory Method. *Handbook of constructionist research* 1 (2008), 397–412. cited on p. 402, 403.

[20] Herbert H Clark. 1996. *Using Language.* Cambridge University Press.

[21] Herbert H Clark and Susan E Brennan. 1991. Grounding in Communication. (1991).

[22] Herbert H Clark and Keith Brown. 2006. Context and Common Ground. *Concise Encyclopedia of Philosophy of Language and Linguistics (2006)* (2006), 85–87.

[23] European Comission. 2023. What are the Responsibilities of a Data Protection Officer (DPO)? Retrieved Mar 13, 2023 from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/data-protection-officers/what-are-responsibilities-data-protection-officer-dpo_en

[24] Zoom Video Communications. 2023. Zoom. Retrieved Mar 13, 2023 from https://zoom.us

[25] North American Electric Reliability Corporation. 2023. North American Electric Reliability Corporation. Retrieved Mar 13, 2023 from https://www.nerc.com

[26] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2019. We Value Your Privacy... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Informatik Spektrum* 42 (2019), 345–346.

[27] Pär Emanuelsson and Ulf Nilsson. 2008. A Comparative Study of Industrial Static Analysis Tools. *Electronic notes in theoretical computer science* 217 (2008), 5–21.

[28] Robert Feldt, Thomas Zimmermann, Gunnar R. Bergersen, Davide Falessi, Andreas Jedlitschka, Natalia Juristo, Jürgen Münch, Markku Oivo, Per Runeson, Martin Shepperd, Dag I. Sjøberg, and Burak Turhan. 2018. Four Commentaries on the Use of Students and Professionals in Empirical Software Engineering Experiments. *Empirical Softw. Engg.* 23, 6 (dec 2018), 3801–3820. https://doi.org/10.1007/s10664-018-9655-0

[29] Office for Civil Rights. 2023. Health Insurance Portability and Accountability Act. Retrieved Mar 13, 2023 from https://www.hhs.gov/hipaa

[30] International Organization for Standardization. 2023. Retrieved Mar 13, 2023 from https://www.iso.org

[31] GDPR Enforcement Tracker. 2023. Statistics: Fines imposed over time. Retrieved Mar 13, 2023 from https://www.enforcementtracker.com/?insights

[32] Google. 2023. Google Ads Policy. Retrieved Mar 13, 2023 from https://support.google.com/adspolicy/answer/6242605?hl=en

[33] Google. 2023. Google Cloud Services. Retrieved Mar 13, 2023 from https://cloud.google.com

[34] Matthew Green and Matthew Smith. 2016. Developers are not the Enemy!: The Need for Usable Security APIs. *IEEE Security & Privacy* 14, 5 (2016), 40–46.

[35] Marco Gutfleisch, Jan H. Klemmer, Niklas Busch, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. 2022. How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, San Francisco, CA, US, 893–910. https://doi.org/10.1109/SP46214.2022.9833756

[36] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by Designers: Software Developers' Privacy Mindset. *Empirical Software Engineering* 23, 1 (2018), 259–289.

[37] Julie M. Haney and Wayne G. Lutters. 2018. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (Baltimore, MD, USA) *(SOUPS '18)*. USENIX Association, USA, 411–425.

[38] Julie M Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. 2018. " We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products.. In *SOUPS@ USENIX Security Symposium.* USENIX Association, Baltimore, MD, USA, 357–373.

[39] Harjot Kaur, Sabrina Amft, Daniel Votipka, Yasemin Acar, and Sascha Fahl. 2022. Where to Recruit for Security Development Studies: Comparing Six Software Developer Samples. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 4041–4058. https://www.usenix.org/conference/usenixsecurity22/presentation/kaur

[40] Mannat Kaur, Michel van Eeten, Marijn Janssen, Kevin Borgolte, and Tobias Fiebig. 2021. Human Factors in Security Research: Lessons Learned from 2008-2018. https://doi.org/10.48550/ARXIV.2103.13287

[41] Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns. 2022. Keeping Privacy Labels Honest. *Proceedings on Privacy Enhancing Technologies* 4 (2022), 486–506.

[42] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

[43] Konrad Kollnig, Lu Zhang, Jun Zhao, and Nigel Shadbolt. 2023. Before and After China's new Data Laws: Privacy in Apps. arXiv:2302.13585 [cs.CY]

[44] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. 2017. "I Have No Idea What i'm Doing": On the Usability of Deploying HTTPS. In *Proceedings of the 26th USENIX Conference on Security Symposium* (Vancouver, BC, Canada) *(SEC'17)*. USENIX Association, USA, 1339–1356.

[45] Thomas D. LaToza, Gina Venolia, and Robert DeLine. 2006. Maintaining Mental Models: A Study of Developer Work Habits. In *Proceedings of the 28th International Conference on Software Engineering* (Shanghai, China) *(ICSE*

'06). Association for Computing Machinery, New York, NY, USA, 492–501. https://doi.org/10.1145/1134285.1134355

[46] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–28.

[47] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 588, 24 pages. https://doi.org/10.1145/3491102.3502012

[48] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2020. The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (2020), 47–64.

[49] Tina Marjanov, Maria Konstantinou, Magdalena Jóźwiak, and Dayana Spagnuelo. 2023. Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR. *Proceedings on Privacy Enhancing Technologies* 3 (2023), 405–417.

[50] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.

[51] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M. Angela Sasse, and Imogen Verret. 2021. Why IT Security Needs Therapy. In *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers* (Darmstadt, Germany). Springer-Verlag, Berlin, Heidelberg, 335–356. https://doi.org/10.1007/978-3-030-95484-0_20

[52] Meta. 2023. Meta. Retrieved Mar 13, 2023 from https://about.fb.com/news/2019/03/protecting-against-discrimination-in-ads

[53] Microsoft. 2023. Microsoft Azure. Retrieved Mar 13, 2023 from https://azure.microsoft.com

[54] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, and Matthew Smith. 2018. Deception Task Design in Developer Password Studies: Exploring a Student Sample. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (Baltimore, MD, USA) *(SOUPS '18)*. USENIX Association, USA, 297–313.

[55] Information Commissioner's Office. 2023. Information Commissioner's Office (ICO). Retrieved Mar 13, 2023 from https://ico.org.uk/

[56] OneTrust. 2023. One Trust. Retrieved Mar 13, 2023 from https://www.onetrust.com

[57] The European Parliament and the Council of the European Union. 2023. A guide to GDPR data privacy requirements. Retrieved Mar 13, 2023 from https://gdpr.eu/data-privacy/

[58] The European Parliament and the Council of the European Union. 2023. Art. 37 GDPR Designation of the Data Protection Officer. Retrieved Mar 13, 2023 from https://gdpr-info.eu/art-37-gdpr/

[59] The European Parliament and the Council of the European Union. 2023. GDPR Chapter 2: Principles. Retrieved Aug 22, 2023 from https://gdpr-info.eu/chapter-2/

[60] The European Parliament and the Council of the European Union. 2023. GDPR Chapter 3: Rights of The Data Subject. Retrieved Aug 22, 2023 from https://gdpr.eu/tag/chapter-3/

[61] The European Parliament and the Council of the European Union. 2023. GDPR Recital 78: Appropriate Technical and Organisational Measures. Retrieved Aug 22, 2023 from https://gdpr.eu/recital-78-appropriate-technical-and-organisational-measures/

[62] The European Parliament and the Council of the European Union. 2023. What is GDPR, the EU's new Data Protection Law? Retrieved Mar 13, 2023 from https://gdpr.eu/what-is-gdpr/

[63] Jonathan Parsons, Michael Schrider, Oyebanjo Ogunlela, and Sepideh Ghanavati. 2023. Understanding Developers Privacy Concerns Through Reddit Thread Analysis. (2023). arXiv:2304.07650 [cs.SE]

[64] Mariana Peixoto, Dayse Ferreira, Mateus Cavalcanti, Carla Silva, Jéssyka Vilela, João Araújo, and Tony Gorschek. 2020. On Understanding How Developers Perceive and Interpret Privacy Requirements Research Preview. In *Requirements Engineering: Foundation for Software Quality*. Springer International Publishing, Cham, 116–123.

[65] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. 2017. Can Security Become a Routine? A Study of Organizational Change in an Agile Software Development Group. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 2489–2503. https://doi.org/10.1145/2998181.2998191

[66] Serena Elisa Ponta, Henrik Plate, and Antonino Sabetta. 2020. Detection, Assessment and Mitigation of Vulnerabilities in Open Source Dependencies. *Empirical Software Engineering* 25, 5 (2020), 3175–3215.

[67] The Open Web Application Security Project. 2023. Retrieved Mar 13, 2023 from https://owasp.org/

[68] Marlene Saemann, Daniel Theis, Tobias Urban, and Martin Degeling. 2022. Investigating GDPR Fines in the Light of Data Flows. *Proceedings on Privacy Enhancing Technologies* 4 (2022), 314–331.

[69] Joni Salminen, Soon-gyo Jung, and Bernard J. Jansen. 2021. Suggestions for Online User Studies. In *HCI International 2021 - Late Breaking Papers: Design and User Experience*, Constantine Stephanidis, Marcelo M. Soares, Elizabeth Rosenzweig, Aaron Marcus, Sakae Yamamoto, Hirohiko Mori, Pei-Luen Patrick Rau, Gabriele Meiselwitz, Xiaowen Fang, and Abbas Moallem (Eds.). Springer International Publishing, Cham, 127–146.

[70] Nikita Samarin, Shayna Kothari, Zaina Siyed, Oscar Bjorkman, Reena Yuan, Primal Wijesekera, Noura Alomar, Jordan Fischer, Chris Hoofnagle, and Serge Egelman. 2023. Lessons in VCR Repair: Compliance of Android App Developers with the California Consumer Privacy Act (CCPA). (2023). arXiv:2304.00944 [cs.CR]

[71] Samsung. 2023. Samsung Business Services Privacy Policy. Retrieved Mar 13, 2023 from https://www.samsung.com/global/business/networks/info/privacy

[72] Awanthika Senarath and Nalin AG Arachchilage. 2018. 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*. ACM, Christchurch, New Zealand, 211–216.

[73] Awanthika Senarath, Marthie Grobler, and Nalin Asanka Gamagedara Arachchilage. 2019. Will They Use It or Not? Investigating Software Developers' Intention to Follow Privacy Engineering Methodologies. *ACM Transactions on Privacy and Security (TOPS)* 22, 4 (2019), 1–30.

[74] Raphael Serafini, Marco Gutfleisch, Stefan Albert Horstmann, and Alena Naiakshina. 2023. On the Recruitment of Company Developers for Security Studies: Results from a Qualitative Interview Study. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. 321–340.

[75] Sean Sirur, Jason R.C. Nurse, and Helena Webb. 2018. Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (Toronto, Canada) *(MPS '18)*. Association for Computing Machinery, New York, NY, USA, 88–95. https://doi.org/10.1145/3267357.3267368

[76] Dag I. K. Sjøberg, Bente Anda, Erik Arisholm, Tore Dybå, Magne Jürgensen, Amela Karahasanovic, Espen F. Koren, and Marek Vokác. 2002. Conducting Realistic Experiments in Software Engineering. In *Proceedings of the 2002 International Symposium on Empirical Software Engineering (ISESE '02)*. IEEE Computer Society, USA, 17.

[77] Sonar. 2023. SonarSource. Retrieved Mar 13, 2023 from https://www.sonarsource.com/products/sonarqube/

[78] Klaas-Jan Stol, Paul Ralph, and Brian Fitzgerald. 2016. Grounded Theory in Software Engineering Research: A Critical Review and Guidelines. In *Proceedings of the 38th International Conference on Software Engineering* (Austin, Texas) *(ICSE '16)*. Association for Computing Machinery, New York, NY, USA, 120–131. https://doi.org/10.1145/2884781.2884833

[79] Alina Stöver, Nina Gerber, Henning Pridöhl, Max Maass, Sebastian Bretthauer, I Spiecker, M Hollick, and D Herrmann. 2023. How Website Owners Face Privacy Issues: Thematic Analysis of Responses from a Covert Notification Study Reveals Diverse Circumstances and Challenges. *Proc Priv Enhanc Technol* (2023).

[80] Ruoxi Sun, Minhui Xue, Gareth Tyson, Shuo Wang, Seyit Camtepe, and Surya Nepal. 2023. Not Seen, Not Heard in the Digital World! Measuring Privacy Practices in Children's Apps. In *Proceedings of the ACM Web Conference 2023* (Austin, TX, USA) *(WWW '23)*. Association for Computing Machinery, New York, NY, USA, 2166–2177. https://doi.org/10.1145/3543507.3583327

[81] Madiha Tabassum, Stacey Watson, Bill Chu, and Heather Richter Lipford. 2018. Evaluating Two Methods for Integrating Secure Programming Education. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. 390–395.

[82] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 693, 15 pages. https://doi.org/10.1145/3411764.3445768

[83] Mohammad Tahaei, Adam Jenkins, Kami Vaniea, and Maria Wolters. 2021. "I Don't Know Too Much About It": On the Security Mindsets of Computer Science Students. In *Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers 9*. Springer, 27–46.

[84] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. *Proceedings on Privacy Enhancing Technologies* 2022, 2 (2022), 114–131.

[85] Mohammad Tahaei, Kopo M Ramokapane, Tianshi Li, Jason I Hong, and Awais Rashid. 2022. Charting App Developers' Journey Through Privacy Regulation Features in Ad Networks. *Proceedings on Privacy Enhancing Technologies* 1 (2022), 24.

[86] Mohammad Tahaei and Kami Vaniea. 2021. "Developers Are Responsible": What Ad Networks Tell Developers About Privacy. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, Article 253, 11 pages. https://doi.org/10.1145/3411763.3451805

[87] Mohammad Tahaei and Kami Vaniea. 2022. Recruiting Participants With Programming Skills: A Comparison of Four Crowdsourcing Platforms and a CS Student Mailing List. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 590, 15 pages. https://doi.org/10.1145/3491102.3501957

[88] Mohammad Tahaei, Kami Vaniea, and Awais Rashid. 2023. Embedding Privacy Into Design Through Software Developers: Challenges and Solutions. *IEEE Security & Privacy* 21, 1 (2023), 49–57. https://doi.org/10.1109/MSEC.2022.3204364

[89] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376768

[90] The Open Web Application Security Project. 2022. OWASP Dependency-Check. Retrieved Mar 13, 2023 from https://owasp.org/www-project-dependency-check/

[91] Tyler W Thomas, Madiha Tabassum, Bill Chu, and Heather Lipford. 2018. Security During Application Development: An Application Security Expert Perspective. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–12.

[92] Martino Trevisan, Traverso Stefano, Eleonora Bassi, Mellia Marco, et al. 2019. 4 Years of EU Cookie Law: Results and Lessons Learned. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (2019), 126–145.

[93] Upwork Global Inc. 2023. Upwork. Retrieved Mar 13, 2023 from https://www.upwork.com/

[94] Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. 2020. Measuring the Impact of the GDPR on Data Sharing in Ad Networks. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (Taipei, Taiwan) *(ASIA CCS '20)*. Association for Computing Machinery, New York, NY, USA, 222–235. https://doi.org/10.1145/3320269.3372194

[95] Christine Utz, Sabrina Amft, Martin Degeling, Thorsten Holz, Sascha Fahl, and Florian Schaub. 2023. Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 5–28.

[96] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212

[97] Christine Utz, Matthias Michels, Martin Degeling, Ninja Marnau, and Ben Stock. 2023. Comparing Large-scale Privacy and Security Notifications. *Proceedings on Privacy Enhancing Technologies* (2023).

[98] Dirk van der Linden, Irit Hadar, Matthew Edwards, and Awais Rashid. 2019. Data, Data, Everywhere: Quantifying Software Developers' Privacy Attitudes. In *Socio-Technical Aspects in Security and Trust: 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers* (Luxembourg, Luxembourg). Springer-Verlag, Berlin, Heidelberg, 47–65. https://doi.org/10.1007/978-3-030-55958-8_3

[99] Charles Weir, Ingolf Becker, and Lynne Blair. 2021. A Passion for Security: Intervening to Help Software Developers. In *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*. IEEE, IEEE, Madrid, Spain, 21–30.

[100] Charles Weir, Sammy Migues, Mike Ware, and Laurie Williams. 2021. Infiltrating Security into Development: Exploring the World's Largest Software Security Study. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. Association for Computing Machinery, Athens, Greece, 1326–1336.

[101] Michael Whitney, Heather Lipford-Richter, Bill Chu, and Jun Zhu. 2015. Embedding Secure Coding Instruction into the IDE: A Field Study in an Advanced CS Course. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*. 60–65.

[102] Khaled Yakdan, Sergej Dechand, Elmar Gerhards-Padilla, and Matthew Smith. 2016. Helping Johnny to Analyze Malware: A Usability-Optimized Decompiler and Malware Analysis User Study. In *2016 IEEE Symposium on Security and Privacy (SP)*. 158–177. https://doi.org/10.1109/SP.2016.18

[103] Thomas Şerban von Davier, Konrad Kollnig, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2023. We Are Not There Yet: The Implications of Insufficient Knowledge Management for Organisational Compliance. arXiv:2305.04061 [cs.CY]

A JOB DESCRIPTION

(Developer) We are looking for software developers who are involved in fulfilling privacy requirements for the software they developed and are comfortable sharing details about the communication process.
As a team of researchers from XXX, we want to explore the communication process between software developers and privacy experts.

(Experts) We are looking for privacy law experts who are working or have worked with development teams in the past.
As a team of researchers from XXX, we want to examine how privacy experts and development teams collaborate in different settings.

(Team Coordinators) We are looking for team leads who are involved in sharing privacy requirements they received from privacy specialists with the software development teams they lead and are comfortable sharing details about the communication process.
As a team of researchers from XXX, we want to explore the communication process between software developers and privacy experts.

(All) What does this job look like?

- Fill out a short questionnaire (5 min)
- Chose a preferred appointment
- Join the online meeting room at the preferred date
- Have a nice conversation with us (60 min)
- Receive payment via Upwork

The online interview will be in English and will last approximately 60 minutes. It is rewarded with an expense allowance of $75. The results will be treated with strict confidentiality and will be published in anonymized and aggregated form. We are not interested in product details or any other confidential information. We would like to examine processes in the company context.

If you have any questions, feel free to contact us. We will provide you with further information.

B SCREENING QUESTIONS

Developer

(1) Have you worked on the user privacy of a software product?
(2) Did you collaborate on privacy tasks with security experts in the past?
(3) Are you willing to talk about the communication process in a specific context/example where privacy requirements were discussed?

Team Coordinators

(1) Have you worked on the user privacy of a software product?
(2) Did you collaborate on privacy tasks with security experts in the past and communicated these requirements to software developers?
(3) Are you willing to talk about the communication process in a specific context/example where privacy requirements were discussed?

Experts

(1) Have you worked on the user privacy of a software product?
(2) Have you provided privacy requirements or guidelines to software development teams?
(3) Are you willing to talk about the communication process in a specific context/example where privacy requirements were discussed?

C DEMOGRAPHICS SURVEY

Q1 How old are you? [Numerical field]

Q2 What is your gender?

- ○ Male
- ○ Female
- ○ Non-binary
- ○ Prefer not to answer
- ○ Other (please specify): ________

Q3 What is the highest level of school you have completed or the highest degree you have received?

- ○ Less than high school / GCSE or equivalent
- ○ High school or equivalent / A level or equivalent
- ○ Some college, currently enrolled in college, or two-year associate's degree, completed part of a higher education course, or currently enrolled
- ○ Vocational degree
- ○ Bachelor's degree
- ○ Some graduate school, or currently enrolled in graduate school
- ○ Master's or professional degree
- ○ Doctorate degree
- ○ Other: ________

Q4 In which country do you currently reside? [Dropdown-list]

Q5 What is your current employment status?

- ○ Employed full-time
- ○ Employed part-time
- ○ Prefer not to answer
- ○ Other: ________

Q6 How many people were employed in the largest company you worked for? (Approximate) [Free text field]
Q7 What is your current job title? [Free text field]
Q8 How many years have you been in the software industry? [Numerical field]
Q9 How many years have you been in the software industry? [Numerical field]
Q10 How many people were employed in the largest company you worked for? (Approximate) [Free text field]
Q11 How many years of experience do you have in your current field? (e.g., 5 years as a software developer) [Free text field]

D INTERVIEW GUIDES

Thank you again for participating in our study. We are interested in how privacy requirements are communicated and implemented in the software development process within your company. To get a better understanding of your company context, could you please elaborate on the following:

(1) **Company context** (All participants)
- What field is your company in?
- How old is your company?
- In which area is the company located?
- Please describe the types of software/products your company creates.
- Who are the customers of the company?
- How many employees does your company have?
- How many software developers are employed in your company?
- Are project managers/team leaders employed at your company?
- Who is responsible for privacy within your company? How many privacy experts are employed in your company?
- What is your role within the company?
- What is your educational background?
- What qualifications are required to accomplish privacy tasks within your work context?
- How many members are there in your team?
- Can you describe what the software development process looks like at your company?
- Which is the primary development process used by your team/the team you work with?
- Please describe the types of software you develop or work on.

(2) **Privacy requirements** (All participants)
- Can you describe your understanding of privacy within your company?
- Can you describe your understanding of privacy within your work context?
- What does it mean to include privacy in the development process within your work context?
- Can you describe the difference between security and privacy? Please elaborate.
- Does your company follow any internal privacy regulations? Please elaborate.
- Does your company follow any external privacy regulations?
- Did you hear about the General Data Protection Regulation (GDPR) passed by the European Union (EU)? Please elaborate.
- Did you hear about the California Consumer Privacy Act (CCPA)? Please elaborate.
- Which privacy concepts come to your mind within your work context?
- Which privacy concepts did you implement within your work context?
- Did you implement Privacy by Design within your work context? Do you know this concept? Where do you know it from?
- Did you implement Fair Information Practices within your work context? Do you know this concept? Where do you know it from?
- Did you implement Privacy Impact Assessment within your work context? Do you know this concept? Where do you know it from?
- Did you implement Data Minimization within your work context? Do you know this concept? Where do you know it from?

For the rest of the interview, when we mention “privacy,” we refer to data protection and data privacy. Data protection means keeping data safe from unauthorized access. Data privacy means empowering your users to make their own decisions about who can process their data and for what purpose. For example, in the context of data minimization, you should collect and process only as much data as absolutely necessary for the purposes specified. Please note that we are not asking about data security where you’re required to handle data securely by implementing “appropriate technical and organizational measures.”

(3) **Communication of privacy requirements** (Developer)
- Who provides the information required to successfully implement privacy requirements?
- Which tasks are you involved in the privacy process?
- What information about the software project do you pass to privacy experts?
- When do you get privacy requirements for the project?
- How are privacy requirements created?
- Do you need to consider any privacy regulations or guidelines within your company when developing software? Please elaborate.
- Do you understand these privacy regulations or guidelines?
- Which format do the privacy requirements have that you get (e.g., checklists, templates)?
- Is essential information missing which helps to implement privacy requirements?
- What does the communication process look like between privacy experts and software developers?
- What does the communication process regarding privacy look like between software developers and team leads?
- Who involves you in the privacy process?
- What person would you contact to get privacy requirements?
- How are the privacy requirements passed to the development teams/management?
- Do you understand the provided privacy requirements?
- How do you implement privacy requirements in the software development process?
- Do you face any issues implementing privacy requirements?
- What would the communication process look like if developers have questions regarding privacy requirements?
- Do you get feedback on the implementation of the privacy requirements? By whom?
- Would someone check the software code for privacy requirement issues?
- What do you like about the communication process between privacy experts and software developers within your company?
- What might improve the communication process between privacy experts and software developers within your company?
- Is there anything related to privacy requirements at your company you would like to talk about?

(4) **Communication of privacy requirements** (Experts)
- When do you get involved in the software development process within your company?
- Who provides the information required to successfully create privacy requirements?
- Which tasks are you involved in the software development process?
- When do you create privacy requirements for the project?
- What information about the software project do you get to create privacy requirements?
- How are privacy requirements created?
- Do you need to consider any privacy regulations or guidelines within your company when creating privacy requirements? Please elaborate.
- Do you understand these privacy regulations or guidelines?
- Which format do the privacy requirements have that you create (e.g., checklists, templates)?
- Is essential information missing which helps create privacy requirements?
- What does the communication process look like between privacy experts and software developers?
- Who involves you in the software development process?
- What person would you contact to provide the privacy requirements?
- How are the privacy requirements passed to the development teams/management?
- Do software developers understand the provided privacy requirements?
- How do software developers implement privacy requirements in the software development process?
- Do software developers face any issues implementing privacy requirements?
- What would the communication process look like if developers have questions regarding privacy requirements?
- Do software developers get feedback on the implementation of the privacy requirements? By whom?
- Would you check the software code for privacy requirement issues?
- What do you like about the communication process between privacy experts and software developers within your company?
- What might improve the communication process between privacy experts and software developers within your company?
- Is there anything related to privacy requirements at your company you would like to talk about?

(5) **Communication of privacy requirements** (Team Coordinators)

- Which tasks are you involved in the privacy process?
- Who provides the information required to successfully implement privacy requirements?
- What information about the software project do you pass to privacy experts?
- When do you get privacy requirements for the project?
- How are privacy requirements created?
- Do you need to consider any privacy regulations or guidelines within your company when developing software? Please elaborate.
- Do you understand these privacy regulations or guidelines?
- Which format do the privacy requirements have that you get (e.g., checklists, templates)?
- Is essential information missing which helps to implement privacy requirements?
- What does the communication process look like between privacy experts and team leads?
- What does the communication process look like between software developers and team leads?
- Who involves you in the privacy process?
- What person would you contact to get privacy requirements?
- How are the privacy requirements passed to the development teams/management?
- Do software developers understand the provided privacy requirements?
- How do software developers implement privacy requirements in the software development process?
- Do software developers face any issues implementing privacy requirements?
- What would the communication process look like if developers have questions regarding privacy requirements?
- Do software developers get feedback on the implementation of the privacy requirements? By whom?
- Would you check the software code for privacy requirement issues?
- What do you like about the communication process between privacy experts and software developers within your company?
- What might improve the communication process between privacy experts and software developers within your company?
- Is there anything related to privacy requirements at your company you would like to talk about?

(6) **Example walkthroughs** (All participants)

- Can you provide a concrete example of a privacy requirement you have created at work?
- What was the reason for creating the privacy requirements? Was it reacting to a change in the legislature?
- For what context were the privacy requirements created?
- Who received the privacy requirements?

Now I would like to discuss fictional scenarios with you. You are given the following requirement from your legal department:

> "The access control must be enabled for the following table: Table_1b" – (Developer, Team Coordinators)

- Is this a privacy requirement that could be implemented within your company?
- What would the communication process between privacy experts and software developers look like for this privacy requirement?
- How would software developers implement this privacy requirement?
- How would the implementation of this privacy requirement be verified?

You are given the following requirement from your legal department:

> "User data stored in the following tables will be retained for a maximum of 30 days after collection: table_1, table_2, table_3" – (Developer, Team Coordinators)

- Is this a privacy requirement that could be implemented within your company?
- What would the communication process between privacy experts and software developers look like for this privacy requirement?
- How would software developers implement this privacy requirement?
- How would the implementation of this privacy requirement be verified?

You are given the following requirement from your legal department:

> "The team's use of model output data will be limited to analytic purposes related to X measurement experiment. Collected data cannot be used for advertising" – (Developer)

- Is this a privacy requirement that could be implemented within your company?
- What would the communication process between privacy experts and software developers look like for this privacy requirement?
- How would software developers implement this privacy requirement?
- How would the implementation of this privacy requirement be verified?

Your company makes the following commitment, and you are tasked to communicate the corresponding privacy requirement to the software developers:

> "Anyone who wants to run housing, employment or credit ads will no longer be allowed to target by age, gender or zip code." – (Experts)

- Is this a privacy requirement that could be implemented within your company?
- What would the communication process between privacy experts and software developers look like for this privacy requirement?
- How would software developers implement this privacy requirement?
- How would the implementation of this privacy requirement be verified?

Your company makes the following commitment, and you are tasked to communicate the corresponding privacy requirement to the software developers:

> "We do not access the microphone just because the app is open, nor do we use it when you are not in the app." – (Experts, Team Coordinators)

- Is this a privacy requirement that could be implemented within your company?
- What would the communication process between privacy experts and software developers look like for this privacy requirement?
- How would software developers implement this privacy requirement?
- How would the implementation of this privacy requirement be verified?
- What else would you like to add that you did not mention during the interview about privacy requirements?

E CODEBOOK

Table 3: Codebook

Category	Description	Example Quote	Code List (Total Frequency/Number of Participants)
Definitions			
Privacy Defintions	Statements that relate to the participants' understanding of privacy. This includes concepts such as accountability, consent, and compliance with laws.	*Within my work context, I would say that privacy and my understanding of privacy is in accordance with legislation, applicable legislation, and that depends where you are.*	Collected Information (8/8), Compliance to Laws (7/5), Consent (7/6), Information Storage (4/4), Human Right (3/3), Sensitive Information (3/3), Purpose Limitation (3/3), Authorized Access (2/2), Satisfying Customers Needs (2/2), Non-Disclosure Agreements (2/1), Accountability (1/1), Competitive Advantage (1/1), Depending on Culture (1/1)
Privacy Concepts	Statements related to the concepts of Privacy by Design, Data Minimization, Fair Information Practices, and Privacy Impact Assessments, as well as privacy concepts participants mentioned themselves.	*I would say data retention is a big one. Sometimes it's kind of like. Some people have issues letting go. Right. So can we just keep this data like we might need it in five years?*	Privacy Impact Assessment (74/30), Fair Information Practice Principles (73/30), Privacy by Design (72/30), Data Minimization (67/30), Consent (14/8), Access Control (13/6), Tracking (9/6), Data Retention (8/7), Transparency (9/6), Compliance (6/6), Honoring Preferences (6/5), Data Staying in EU (6/4), Internal Privacy Policy (6/4), Purpose Limitation (6/4), Anonymity (4/2), Accountability (3/2), Control over Data (2/1), Data Collecting (2/1), Legitimate Interest (2/1), Data Integrity (1/1), Data Loss (1/1), Data Processing (1/1), Data Subject Rights (1/1), Sensitive Data (1/1)
Security Focus	Statements that participants made on topics that are closely related to security issues when asked about privacy. This includes encryption, worries about attackers, and authentication.	*So personally, it feels like a concept that I feel [...] is one thing that embraces that for me, like with encryption, it really knocks out all privacy concerns. So it's something I've done and it makes life easy for me, basically.*	Security Mechanisms (31/10), Encryption (27/13), Data Security (23/12), Concern About Attacks (12/8), Authentication (10/6), Privacy and Security One Concept (5/3), Privacy Component of Security (4/4)
Guidelines			
Company Internal Guidelines	Statements related to company internal guidelines focused on privacy used by participants. Examples include templates, documentation, and manuals.	*So, yeah, we do have that private privacy by design policy. We also have the data subject rights policy, a data breach protocol. We have data retention, working instructions. And we also. Kind of related to the vendor management policy, which is also useful for us to make sure that all of our vendors are compliant so that we have.*	Privacy Policies (22/15), Questionnaires (13/3), Documentation (11/10), Non-Disclosure Agreements (6/3), Templates (4/3), Frameworks (4/1), Technical Specifications (3/3), Standards (2/2), Informal (2/1), Manual (1/1)
External Guidelines	Statements related to external guidelines focused on privacy used by participants. Examples include guidelines from NIST, ISO, and user-created blog posts, as well as regulations like the GDPR or CCPA.	*Generally, my guide by default is GDPR. However, some other clients have specific compliance or specific requirements beyond the jurisdiction of the UK or GDPR.*	**Regulations:** GDPR (82/22), Regional Laws (22/11), HIPAA (24/5), Laws (13/10), CCPA (12/9), UK GDPR (6/3) ADA (3/3), PCI (3/2), Australian Privacy Act (2/2), Data Privacy Act (2/1), Data Protection Act (2/1), FDPA (2/1), Gambling Legislation (2/1), Freedom of Information Act (1/1), APP (1/1), ENGA (1/1), Finance Regulations (1/1), LGPD (1/1), NERC CIP (1/1), PIPEDA (1/1), Safe Habor (1/1) **Other:** ISO (6/4), OWASP Top Ten (3/2), SOC (3/2), NIST (3/1), Examples (2/2), ICO (2/1), KYC (2/1), ENISA (1/1), European Data Protection Board (1/1), FDIC (1/1), FINRA (1/1), GRC (1/1), GSMA (1/1), Industry Standards (1/1), Ofcom (1/1), Online Resources (1/1), User Blogs (1/1)
Communication			
Involved Persons	Statements concerning people involved in the communication process. Examples include developers, legal personnel, and management positions.	*So it was much faster to be able to communicate the changes, but generally, the process flow would be that they'd go to the business owner so that whatever the marketing executive or the customer experience executive, and then they would come down to the legal team to ask for DPO opinion.*	Developer (158/24), Leadership Position (92/27), Lawyer (68/16), Management (52/16), Clients (37/11), Security (27/9), Privacy Department (18/9), DPO (16/6), Stakeholder (14/3), QA (13/8), Third-Party Lawyer (6/6), Designer (6/4), Analysts (4/3), Government Body (4/2), Marketing (3/2), HR (3/2), Sales (3/2), Everyone Involved (2/1), Software Architect (2/1), DevOps (1/1), Senior Engineer (1/1)
Exchanged Information	Statements concerning information that are exchanged during the communication process. Examples include product requirement documents, product descriptions, and software demos.	*And then if there's any advice, they'll try to put it into something that resembles a PRD, but usually just some sort of comments that they'll leave.*	**To Privacy Experts:** What Data is Collected (32/18), Product Description (16/9), Measures in Place (15/9), Storage of Information (14/11), Information Usage (13/10), Data Handling (8/6), Questionnaires (6/4), Involved Parties (4/3), Risk Assessment (3/2), Technical Requirements (2/2), User Flow (1/1), Software Demo (1/1), Existing Privacy Policies (1/1) **To Development Teams:** Recommendations (34/17), Risk Assessment (30/10), Privacy Policies (10/6), Checklists (9/8), Privacy Decision Document (8/5), Mitigations (7/6), Questionnaire (7/6), Product Requirement Document (6/4), Risk Score (5/4), Templates (2/2), Call Recordings (1/1)
Communication Tools	Statements concerning tools used for communication. Examples include ticket systems, Zoom, and Confluence.	*We have a tool that is JIRA, basically, and we communicate that through JIRA. So they open an issue on JIRA to the legal project, describing their doubts or what they are doing, what they are preparing, and all what they think is relevant. And then we answer in writing.*	Tickets (16/8), Slack (5/3), Google Docs (2/2), OneTrust (2/2), Conferencing Tools (1/1), Confluence (1/1), SharePoint (1/1), Zoom (1/1)
Starting Point	Statements concerning the start time of the communication process. Examples include from the beginning, before release, and never.	*Well, I don't really get requirements at all. [...] Like they don't tell me anything. They just kind of say, "Do this" and expect me to [...] decide myself what the privacy levels should be.*	Beginning (46/21), Upon Request (10/8), During Development (8/7), After Deployment (6/5), Before Release (6/4), Testing Phase (6/6), During Sprints (5/4), Never (2/2)
Implementation			
Verification	Statements on the verification process that participants described. This includes the time of verification, the process used to verify privacy requirements, and the persons involved.	*That type of Verification probably wouldn't be done. Yeah, I don't imagine that it is. [...] The most that would be tested is access control [...]*	**Process:** No Verification (13/10), Assessment (12/8), Functional Tests (8/3), Trust (6/6), Code Checks (5/5) **Time of Verification:** Regular Audits (7/6), Before Going Live (2/2), After Implementation (1/1), Once Live (1/1) **Person Conduction:** QA (13/7), Developers (10/5), Team Coordinator (4/3), Consulting Group (4/2), Legal Team (2/2), Info-Sec (2/2), Clients (1/1), Whoever Created the Requirement (1/1)

Table 3: Codebook (continued)

Category	Description	Example Quote	Code List (Total Frequency/Number of Participants)
Implementation			
Tools	Statements related to tools used during the implementation of privacy requirements. This can be software used during the development and public information used to guide developers during the implementation. It does not include tools used specifically for communication.	*And since we use GCP like the Google Cloud platform, it's actually quite easy to set these limits because when you add it, you just need to well, you can for a table itself, you can give a limit for how long Items can stay in that table and then it's all just kind of automated.*	Amazon Web Services (9/3), Azure (2/2), OneTrust (2/2), Google Cloud (2/1), CNIL DPIA Tool (1/1), Git (1/1), GRC Tools (1/1), Very Good Security (1/1)
Motivation for implementing privacy	Statements that clarify the reason participants have for implementing privacy requirements into the software. This can be, for example, personal motivation, wishes from customers, or trying to be compliant with legislation.	*Maybe it's important because sometimes our clients contact us not because they want to ensure the privacy compliance of their product, but they are required to do so, for example, by a marketplace or [...] they want to be certified or they want to get a big client, for example, some software development team that offers software for banks.*	Compliance (22/15), Customer Wishes (17/8), Fines (9/9), Bad PR (9/6), Pass Audit (7/3), Getting Sued (6/6), Right Thing to Do (1/1), Work Consequences (1/1)
Good Practices			
Communication	Statements that relate to positive factors mentioned by participants that would help communication. Examples are open communication, starting early, and good communication tools.	*I think that we can start the communication at an early stage of the process because sometimes they come to us when they have already worked on something. For example, the recording marketing solution was quite already in place and finally, we had to say, no, you cannot do this because we are not able to treat this kind of data too much.*	Open Communication (25/13), Starting Early (10/8), Better Communication Tools (6/2), More Context (5/3), Proactive Communication (5/4), Clear Instructions (4/3), Everyone Involved (4/4), Understanding from Both Sides (3/3), Clarify Legal Terms (2/2), Documentation (1/1), Assess Worst-Case Scenario (1/1)
Company context	Statements concerning factors perceived as positive by participants within a company context. Examples are experienced colleagues, awareness, and training.	*I think one of them comes from a privacy background, from a large, kind of data company in the US. And so I think that experience helps a lot because I think they go within the engineering squad, they go to that particular individual.*	Training (23/11), Awareness (17/11), Experienced Colleagues (17/12), Company Culture (8/5), Experience (5/5), Resources for Privacy (3/2), Third Party Responsible For Privacy (3/3), Collaboration (2/2), Internal Audits (2/2)
Implementation	Statements relating to helpful factors during the implementation of privacy requirements. Examples are good tools, good examples, and regular testing.	*It's again, it comes to, like I said, with GDPR, the person who did it first is going to struggle. But as long as there is a precedent, the ones that come after that, it's much easier for them.*	Examples (8/5), Clear Instructions (7/6), Better Tools (3/2), Lower Data Collection (2/2), Professional Guidelines (2/2), Regular Testing (2/2), Documentation (1/1), Code Reviews (1/1)
Challenges			
Communication	Statements related to challenges participants experienced during the communication process of privacy requirements. This includes all communication between the three groups as long as they relate to privacy.	*Technical information I feel is always missing. The client more often than not doesn't know. You know what? Technical requirements are being implemented. You know, and for some reason, I find that they either don't wish to know or they're happy to just put a very general paragraph to do with that or they don't ask.*	Legal Terms Unclear (15/11), Lack of Communication (12/9), Privacy seen as Disruptive (12/8), Missing Information (7/7), Privacy Expert not Technical (7/5), Communication is Hard (5/4), Late Requirements (5/3), Expert not Reachable (4/2), Number of Regulations (3/3), Missing Resources (2/2), Changing Requirements (1/1)
Company context	Statements related to issues that arise from the company context. Examples include a lack of responsibilities, resource problems, and data use by different departments.	*And other than that, it's very difficult because startups do not have that much budget to look into these concepts, to hire a particular expert. And in fact, most of the startups, they do not have a privacy person, so they do not have a security person as well.*	Privacy not Priority (29/14), Resource Problem (11/7), Third Parties (11/9), Regional Differences (10/6), Human Error (8/7), Lack of Responsibility (8/7), Lack of Teamwork (8/3), Data used by Different Department (7/5)
Implementation	Statements that concern challenges during the implementation phase of privacy requirements. These may include issues such as conflicting requirements, complex systems, and misunderstandings of requirements.	*So there are a lot of scenarios that are not directly covered inside the explaining regulation, and that's where the back and forth with the regulating body comes because you need to give them examples. What if this, what if that, will that be compliant to you?*	Lack of Understanding (16/9), Complex Systems (15/11), Vague Guidelines (9/7), Changing Systems (5/4), Conflicting Requirements (3/3), Displaying Information to User(2/2)