# Mapping Privacy Responsibilities in Agile Development

Yunze Zhao
University of Maryland

Chandler Wang
University of Maryland

Yibo Zhao
University of Maryland

## CCS Concepts

• **Privacy**; • **Agile Development**; • **Software Development**; • **Privacy Engineering**;

**ACM Reference Format:**
Yunze Zhao, Chandler Wang, and Yibo Zhao. 2024. Mapping Privacy Responsibilities in Agile Development . In . ACM, New York, NY, USA, 9 pages. https://doi.org/XXXXXXX.XXXXXXX

## 1 Introduction

Agile project management has gained widespread acceptance in software development due to its ability to enhance communication, accelerate development cycles, and improve flexibility in responding to changing requirements [13] [14] [1]. The Agile framework encourages iterative progress, regular feedback, and close collaboration among team members, which generally benefits software quality and user satisfaction. However, this rapid pace of development often sidelines critical non-functional requirements, such as privacy and security, which are less immediately visible but equally important [13] [1].

While the roles of product managers and developers in Agile teams are well-defined in terms of feature prioritization and software delivery [19] [20], there remains a significant gap in accountability when it comes to addressing privacy concerns. Unlike traditional software development, where responsibilities may be more rigidly assigned, Agile teams operate in a more fluid environment. This often results in ambiguity around who is responsible for addressing privacy-related problems that would occur during the development. [19]. Moreover, with differing privacy laws across regions, such as GDPR in Europe or CCPA in California, developers and product managers alike face challenges in navigating complex regulatory landscapes even with the helps of legal teams. [12]. These laws require organizations to not only ensure compliance but also implement privacy by design, a principle that requires developers to integrate privacy considerations throughout the development process [21].

Despite this legal and ethical imperative, developers are frequently left without clear guidance on how to operationalize privacy requirements during Agile sprints. Privacy concerns often do not appear as explicit and urgent user stories or backlog items, leaving developers to focus on functional requirements of the products without fully considering and addressing privacy implications [2] [19]. Meanwhile, project managers tend to prioritize delivery timelines, feature development, and overall project progress, which can lead to privacy considerations being deprioritized or overlooked entirely [20] [19]. This lack of ownership often leads to gaps in privacy protection, increasing the risk of data breaches or non-compliance with privacy regulations [12].

Having this gap in mind, this study aims to shed lights on the following key questions:

- Who should take ownership of privacy concerns within an Agile development team
- At what stage of the Agile development cycle privacy concerns should be addressed
- How teams can ensure that privacy risks are identified and mitigated early

By providing insights to these questions, this study aims to clarify the roles and processes that are required to embed privacy into the Agile workflow, ensuring that privacy is proactively managed throughout the software development life cycle. Establishing clearer accountability for privacy tasks and identifying privacy concerns early will contribute to better privacy outcomes and reduced risks of security breaches.

## 2 Methods

### 2.1 Recruitment

Participants were recruited from multiple sources, including alumni of the University of Maryland (UMD) who completed CMSC389P and are currently working as product managers. Additional participants were identified through social media platforms such as X (formerly Twitter) and Reddit, as well as personal networks via snowball sampling.

Recruitment announcements outlined the study's purpose, described the semi-structured interview process, and detailed the offered compensation. To ensure legitimacy, potential participants recruited through social media were subject to pre-screening questions to verify their professional background. Ultimately, three participants were recruited through social networks and snowball sampling, while one participant was recruited from the UMD alumni pool.

### 2.2 Pre-Screening Survey

To ensure that participants met the eligibility criteria, a pre-screening survey was distributed across social media platforms along with the recruitment announcement. The survey required potential participants to confirm their current role as project managers and a minimum of one year of experience in project management. Additionally, participants were asked to upload their LinkedIn profiles to validate their professional credentials.

Beyond verification, the pre-screening survey gathered background information on participants' experience and responsibilities


*Conference'17, July 2017, Washington, DC, USA*

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/XXXXXXX.XXXXXXX

in project management to provide context for the interviews. A full list of survey questions is included in the appendix.

## 2.3 Interview Design

Participants took part in a semi-structured interview designed to explore their experiences and perspectives on privacy integration within Agile development workflows. The semi-structured format allowed us to follow a predetermined protocol of themes and main questions while adapting follow-up queries to the individual context of each participant. Each interview lasted approximately thirty minutes, balancing structure with flexibility to capture nuanced insights.

**Interview Structure:** The interview questions were categorized into six key sections, ensuring comprehensive coverage of relevant themes:

- **Team Roles and Responsibilities:** Exploring participants' roles within Agile teams and their interactions with privacy-related tasks.
- **Development Process and Decision-Making:** Examining how teams prioritize tasks and address privacy within the broader development workflow.
- **Identifying and Addressing Risks:** Investigating how privacy risks are identified and mitigated at different stages of development.
- **Integration of Non-Functional Requirements:** Assessing the role of privacy as a non-functional requirement alongside other priorities like security and scalability.
- **Opportunities for Improvement:** Gathering participants' suggestions for improving privacy integration and Agile workflows.
- **Integration for Privacy Development:** Understanding how teams handle user privacy concerns and compliance with regulations like GDPR and CCPA.

**Interview Design Process:** To ensure alignment with the study's objectives, the interview questions were carefully crafted based on the following principles:

- Covering key areas identified in prior literature, such as privacy ownership, timing, and risk management.
- Encouraging participants to share detailed examples to provide rich qualitative data.
- Balancing open-ended questions to allow participants to elaborate while ensuring specific insights on privacy practices.

The full list of interview questions can be found in the appendix.

**Compensation and Participation:** Upon completing the interview, participants were offered a $20 Amazon gift card as a token of appreciation. However, three of the four participants declined compensation due to their organizations' policies.

This interview design ensured a structured yet adaptable framework for capturing diverse perspectives on privacy integration within Agile workflows, providing valuable insights for the study.

## 2.4 Ethics

This study was reviewed and approved by the University of Maryland Institutional Review Board. We obtained informed consent including for being recorded and automatic transcription of the recorded audio. We ensured that they understand the nature of the study, how their data will be used and protected, and that they have the right to withdraw. Finally, we anonymized the data during data analysis and reporting and omit any identifiable information.

## 2.5 Analysis

The analysis focused on transcripts generated from audio recordings of the semi-structured interviews. A local Large Language Model (LLM) was used to transcribe the recordings, followed by manual corrections to ensure accuracy. Once the transcripts were finalized, qualitative data coding was performed to identify and analyze key themes.

For the coding process, two researchers independently coded all transcripts to ensure reliability and minimize bias. After an initial round of coding, the researchers collaboratively developed a set of initial codes to ensure consistent interpretation of the data. The analysis involved two iterative rounds of coding. During the first round, the focus was on identifying preliminary themes and patterns in the data. In the second round, these themes were refined and confirmed to ensure alignment with the study's objectives.

To maintain flexibility and responsiveness, the analysis approach was revisited and adjusted as new data emerged. The final code book is included in the Appendix.

# 3 Limitations

Due to the limited sample size, our study may not be generalizable to all Agile teams. Our results may also be affected by demand characteristics, where participants are inclined to answer positively due to close interaction with the interviewers. We framed our questions in a neutral way to mitigate this bias. We may also experience some self-selection bias. The recruitment messages explain that the study involves risk management in an Agile development setting. This may disproportionately attract individuals who are more cognizant of risks such as privacy.

Another key limitation of this study is the influence of company size and structure on privacy practices. Larger organizations often compartmentalize privacy responsibilities, while smaller teams may face resource constraints, resulting in varied challenges and approaches. Future research should narrow its scope to explore specific organizational contexts to better understand how size and structure impact privacy integration.

Furthermore, due to time and budget constraints, we focus exclusively on interviewing product managers. As a result, we were unable to collect insights from other key roles in the Agile team, such as developers or scrum masters. Information from these members could provide a more comprehensive view of how privacy concerns are managed in different roles. Our insights will primarily serve as suggestions and may not be applicable to all Agile teams, especially those operating in industries with specific needs, such as medical software or sectors requiring more stringent privacy considerations.

# 4 Related Work

## 4.1 Privacy Gaps

Addressing non-functional requirements (NFRs), such as privacy, remains a persistent challenge in Agile Software Development (ASD). Agile's focus on rapid, iterative delivery often deprioritizes privacy, complicating regulatory compliance and eroding user trust [16]. Studies highlight that ASD lacks mechanisms for ensuring compliance with regulations like GDPR, CCPA, and Brazil's LGPD, creating significant gaps in integrating privacy requirements early in development [4, 16].

Proposed frameworks aim to embed regulatory requirements into Agile workflows. Chukwurah et al. advocate for iterative feedback loops and cross-functional collaboration to foster proactive privacy practices [4]. Similarly, Canedo et al. demonstrate how user stories and feedback can elicit privacy requirements but note limited adoption of privacy-specific tools, emphasizing the need for better training and resources [3]. Wagner and Ford propose privacy metrics to monitor compliance without sacrificing Agile adaptability, helping teams balance privacy with Agile's flexibility [22].

Collignon et al. suggest selective information sharing over total transparency to balance privacy with team dynamics, aligning with communication privacy management (CPM) theory [5]. This approach helps project managers negotiate transparency and privacy needs effectively. However, resource-constrained environments, such as startups, often deprioritize privacy due to limited expertise and the pressure for rapid deployment, as highlighted by Kekulluoglu et al. [8].

While existing models provide insights into privacy compliance and metric-based monitoring, gaps remain in practical, accessible tools for project managers. Future research should focus on context-sensitive strategies to embed privacy responsibilities seamlessly within ASD, particularly for smaller organizations and startups.

## 4.2 Expected Responsibilities

ASD often encourages teams to be more self-sufficient, which calls into question the exact role of a project manager. Studies have investigated the responsibilities a project manager takes on in an Agile team. There is some ambiguity in the exact role that a project manager plays, which often leads to confusion within a team. However, previous work also notes some important responsibilities that are expected of a project manager.

Nkukwana and Terblanche [15] found that the role of a project manager is unclear. Implementation and management teams have opposite expectations of the level of direct influence a project manager should exercise. Hoda and Murugesan [7] found that team members in an Agile work environment often lacked guidance and coordination. Langholf and Wilkens [11] had similar findings, discovering that the increased independence of an Agile team led to less organization and empowerment. The results of these studies brought into question the exact roles and responsibilities of an Agile project manager. Shastri et al. [18] specifically investigated the responsibilities project managers in Agile teams take on. They found that project managers were expected to negotiate project details with clients, as well as mentor team members by explaining project details to them.

These studies demonstrate that the Agile approach can cause confusion and disarray without some form of structure. Project managers can provide guidance, but the exact responsibilities of a project manager are often unclear. There are some expectations that a project manager will mentor, guide, and stabilize the team, but their level of involvement is not well-defined. It is important to investigate how Agile project managers navigate and delegate the vital, complex responsibility of privacy amidst deadlines and customer demands.

## 4.3 Developer Confusion in Privacy Engineering

Developer confusion around privacy engineering is a critical challenge in ASD, where the prioritization of rapid iterations and functional requirements often leaves privacy overlooked. Limited training, inconsistent definitions, and a lack of structured processes exacerbate this issue, particularly in environments that conflate privacy with security or deprioritize it due to organizational and project pressures. Researchers have examined the reasons of this confusion and its implications for privacy integration in Agile workflows.

Keküllüoğlu and Acar [9] observed that developers in startups frequently neglect privacy during early development phases, misinterpreting it due to the absence of clear definitions and structured guidelines. Prybylo et al. [17] found that many developers lack formal privacy education, relying on self-teaching, which fosters misunderstandings of key privacy concepts. Kostova et al. [10] highlighted the misalignment between academic privacy solutions and Agile practices, leaving developers without effective strategies to address privacy responsibilities. Hadar et al. [6] noted that developers tend to view privacy narrowly, focusing on external security rather than comprehensive privacy management, an outlook shaped by organizational climates that deprioritize privacy.

These investigations highlight a disconnect between academic privacy solutions and real-world Agile practices, while emphasizing the need for organizational shifts to prioritize privacy education and foster a "privacy mindset" among developers. Addressing this gap is essential to equipping developers with the knowledge and resources necessary to meet privacy obligations in fast-paced, iterative development environments.

# 5 Results

Through interviews with participants occupying various roles in Agile teams, we identified key themes related to privacy ownership, the timing of privacy discussions within development cycles, and strategies for identifying and mitigating privacy risks. These findings highlight the complexities of balancing privacy with Agile's core principles of iterative delivery and responsiveness, shedding light on both current practices and areas for improvement. Below, we present the results organized around the major themes that emerged from our analysis.

## 5.1 Key Privacy Challenges in Agile Teams

Participants identified several challenges related to integrating privacy into Agile workflows. These challenges highlight gaps in responsibility, prioritization, understanding, and risk management,

which often hinder effective privacy practices.

**Shifted Responsibility:** Teams frequently rely on centralized systems or third-party toolkits, assuming privacy concerns are handled externally. This shifted responsibility creates a disconnect, as team members are not directly involved in addressing privacy issues. P1 reflected this sentiment, stating, "We focus more on protecting the company's confidential information rather than addressing broader privacy concerns."

**Low Priority:** While participants acknowledged the importance of privacy, it is often deprioritized during sprint planning. Functional deadlines and immediate deliverables typically take precedence, leaving privacy discussions sidelined until later stages of development.

**Knowledge Gaps:** Participants revealed limited understanding of the data collected by third-party tools or centralized systems. This lack of transparency and knowledge can lead to unintentional privacy risks. P4's request for clarification on privacy definitions during the interview underscores this gap: "I use security and privacy interchangeably. When issues similar to this arise, I would refer to our security team."

**Inaction on Risks:** Although privacy risks, such as user behavior tracking, are recognized, participants noted that these risks are rarely addressed due to limited resources or unclear responsibilities. Without a structured approach or dedicated privacy roles, teams often overlook potential vulnerabilities until they become pressing issues.

These findings highlight the need for greater accountability, education, and structured frameworks to ensure privacy concerns are consistently addressed within Agile teams.

## 5.2 Ownership of Privacy Concerns

Participants revealed a notable disparity in addressing privacy concerns within Agile development processes. While P2 and P3 expressed a sense of responsibility for privacy, they acknowledged the absence of frameworks or protocols explicitly tying these concerns to their workflows. This lack of structured guidance often left them addressing privacy issues on an ad hoc basis.

In contrast, participants from larger organizations (P1 and P4) indicated that privacy responsibilities are heavily compartmentalized within their companies. These tasks are typically managed by dedicated teams or centralized systems, resulting in limited direct engagement with privacy concerns by Agile teams themselves.

Interestingly, project managers in smaller organizations (P2 and P3) demonstrated greater awareness of privacy issues, frequently reflecting on these concerns as part of their development processes. This distinction underscores the influence of organizational context on how privacy responsibilities are perceived and managed, with smaller teams shouldering more direct accountability for privacy-related decisions.

## 5.3 Identifying and Mitigating Privacy Risks

Participants consistently emphasized the importance of adopting a privacy-focused mindset during the planning phase to effectively identify potential risks. P4 specifically noted that treating privacy as a feature during the planning stage allows teams to incorporate actionable targets and insights into their workflows. This proactive approach ensures privacy concerns are not overlooked in the early stages of development.

Despite the absence of consistent privacy discussions during the planning phase, all participants acknowledged that privacy concerns inevitably arise during the development cycle. Participants reported addressing these concerns based on their severity, employing different approaches depending on organizational context and available resources.

To mitigate privacy risks, participants employed varied strategies:

- **Collaboration with Experts:** P4 highlighted the value of involving specialized teams, such as privacy or security teams, to assess and address privacy concerns effectively.
- **Self-Assessment:** P2 and P3, working in smaller organizations, relied on internal team assessments to evaluate and resolve privacy risks.
- **Toolkits and Systems:** P1 reported leveraging company-provided toolkits and centralized privacy systems, assuming these were sufficient to handle privacy concerns.

These findings reveal a diverse range of approaches to identifying and mitigating privacy risks, influenced by team structure, organizational resources, and the availability of specialized support.

## 5.4 Opportunities to Improve

When asked about potential improvements to better identify and mitigate privacy concerns, participants highlighted several common themes. Proper training and references during onboarding were universally mentioned as essential for fostering a privacy-focused mindset among team members. Participants noted that early education on privacy concepts could lay the groundwork for addressing concerns throughout the development lifecycle.

**Specialized Support:** P1, P2, and P3 emphasized the value of having access to privacy experts, such as privacy engineers or consultants, to build confidence in identifying and mitigating privacy issues effectively. P4 further suggested the establishment of a dedicated privacy team to collaborate with development teams, providing necessary resources and support when challenges arise.

**AI-Powered Tools:** Both P2 and P3 identified AI-powered tools as a promising avenue for improving privacy practices. P2 proposed an AI chatbot or scanning tool to analyze planned features and flag potential privacy concerns during the planning phase. This proactive measure would allow teams to address issues before implementation.

**Enhanced Development Practices:** Some participants suggested improvements in coding practices as a means of addressing privacy risks. Specific recommendations included:

- Writing detailed pull request comments to specify the data being collected by new features.
- Providing clear documentation for external users, outlining the data capabilities of APIs or features.

These suggestions highlight the importance of transparent communication and documentation in mitigating privacy risks effectively.

**Privacy as a Feature:** Participants, particularly P4, highlighted that adopting a privacy-focused mindset and treating privacy as a feature to implement can transform ambiguous privacy goals into actionable insights. By embedding privacy into feature design during the planning phase, developers gain clearer objectives and practical steps for ensuring compliance and mitigating risks.

P2 mentioned that having a structured framework or workflow that integrates privacy as a goal of implementation helps teams better understand proactive measures to prevent privacy issues.

Additionally, all participants emphasized the importance of discussing privacy during the planning phase. They noted that privacy is often deprioritized or left out of discussions due to tight timelines and unclear goals. Ensuring that privacy becomes a standard part of sprint planning was identified as a critical improvement to address these challenges effectively.

These opportunities highlight a desire for structured training, expert guidance, innovative tools, and a privacy-as-a-feature approach to integrate privacy considerations more seamlessly into Agile workflows.

## 6 Discussion

This study highlights several challenges and opportunities for integrating privacy considerations into Agile development workflows. Our findings suggest that privacy is often de-prioritized or treated as a secondary concern, particularly in larger organizations where responsibilities are compartmentalized. While centralized systems and third-party tools provide some degree of privacy management, they also create a disconnect, leaving Agile teams with limited understanding of privacy practices and risks.

Several participants noted a lack of structure for dealing with privacy-related issues. Privacy is often seen as abstract, and it is difficult to know when something is a genuine privacy concern. For example, some teams struggled to identify the amount and type of user data that is considered acceptable to collect. Since teams are uncertain on exact specifications, privacy problems are often simply overlooked. Some participants wished for clearer privacy guidelines. Standardized guidelines to make privacy less ambiguous could allow Agile teams to be more structured and efficient in their approach towards privacy.

Participants emphasized the importance of fostering a privacy-focused mindset during the planning phase. Treating privacy as a feature not only provides actionable insights but also ensures that privacy concerns are addressed proactively rather than reactively. However, resource constraints and tight deadlines frequently hinder these discussions. Better privacy guidelines and education could help Agile teams set clearer privacy goals during the planning stage. Structural and cultural changes in Agile workflows could also help prioritize privacy during development. Current Agile teams have a significant focus on functional requirements and deadlines, which overshadow privacy considerations. Widening this focus could make room for important non-functional requirements such as privacy.

Several potential improvements were identified, including the integration of AI-powered tools, enhanced coding practices, and educational resources. Tools that can flag privacy risks during planning and development phases were particularly valued by participants, as they can help bridge knowledge gaps and reduce reliance on external systems. Participants also suggested the inclusion of privacy experts or dedicated teams to guide Agile teams in identifying and mitigating privacy concerns.

The challenges in balancing privacy with functionality, scalability, and other non-functional requirements remain significant. Smaller organizations, in particular, face difficulties in prioritizing privacy due to limited resources and expertise. This underscores the importance of providing accessible frameworks and workflows to embed privacy into Agile practices seamlessly.

### 6.1 Future Work

Future research could explore usability studies to evaluate whether the integration of privacy-focused tools, frameworks, or educational resources improves teams' privacy mindset and practices. Such studies could provide actionable insights into the effectiveness of proposed solutions, such as AI-powered tools or privacy-specific training, in enhancing Agile workflows.

Moreover, investigating cross-functional dynamics within Agile teams, particularly how different roles collaborate on privacy-related tasks, would shed light on the holistic challenges of embedding privacy into workflows. Exploring longitudinal studies to assess the long-term impact of integrating privacy considerations into Agile practices would also be valuable for understanding sustained improvement and compliance with privacy regulations.

Our findings align with prior literature on challenges in Agile workflows, reinforcing the need for proactive measures and structured support to address problems effectively. Future work should explore the implementation of these proposed solutions, such as privacy-focused frameworks and AI-driven tools, to evaluate their impact on Agile teams and their ability to manage privacy responsibly.

## 7 Conclusion

Our results find several challenges for incorporating privacy into Agile workflows. Privacy is a vague and abstract concept to many teams, causing privacy concerns to be put aside and overlooked. Agile teams can often rely on centralized systems or third-parties to ensure privacy. Privacy is given lower priority than immediate deadlines and functional requirements, delaying privacy discussions until late in the development cycle. It can also be unclear which members of an Agile team are responsible for ensuring privacy. Several proposed solutions may be of use. Privacy specialists, AI-powered tools, more thorough coding practices, and implementing privacy as a feature may help Agile teams be more efficient and effective in addressing privacy concerns.

## References


[1] Pekka Abrahamsson, Outi Salo, Jussi Ronkainen, and Juhani Warsta. 2017. Agile Software Development Methods: Review and Analysis. *CoRR* abs/1709.08439 (2017). arXiv:1709.08439 http://arxiv.org/abs/1709.08439

[2] Atheer Aljeraisy, Masoud Barati, Omer Rana, and Charith Perera. 2021. Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. *ACM Comput. Surv.* 54, 5, Article 102 (May 2021), 38 pages. https://doi.org/10.1145/3450965

[3] Edna Dias Canedo, Angelica Toffano Seidel Calazans, Ian Nery Bandeira, Pedro Henrique Teixeira Costa, and Eloisa Toffano Seidel Masson. 2022. Guidelines adopted by agile teams in privacy requirements elicitation after the Brazilian general data protection law (LGPD) implementation. *Requir. Eng.* 27, 4 (Dec. 2022), 545–567. https://doi.org/10.1007/s00766-022-00391-7

[4] Excel G Chukwurah et al. 2024. Agile privacy in practice: integrating CCPA and GDPR within agile frameworks in the US tech scene. *International Journal of Scientific Research Updates* 7, 2 (2024), 024–036.

[5] Stephane Eric Collignon, Salman Nazir, and Nanda Chingleput Surendra. [n. d.]. Agile Systems Development: Privacy Theoretical Lens to Challenge the Full Information Disclosure Paradigm. 59, 6 ([n. d.]), 103679. https://doi.org/10.1016/j.im.2022.103679

[6] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. [Journal First] Privacy by Designers: Software Developers' Privacy Mindset. In *2018 IEEE/ACM 40th International Conference on Software Engineering (ICSE)*. 396–396. https://doi.org/10.1145/3180155.3182531

[7] Rashina Hoda and Latha K. Murugesan. 2016. Multi-level agile project management challenges: A self-organizing team perspective. *Journal of Systems and Software* 117 (2016), 245–257. https://doi.org/10.1016/j.jss.2016.02.049

[8] Dilara Keküllüoğlu and Yasemin Acar. [n. d.]. *"We Are a Startup to the Core": A Qualitative Interview Study on the Security and Privacy Development Practices in Turkish Software Startups.* https://doi.org/10.48550/arXiv.2212.08396 arXiv:2212.08396

[9] Dilara Keküllüoğlu and Yasemin Acar. 2022. "We are a startup to the core": A qualitative interview study on the security and privacy development practices in Turkish software startups. arXiv:2212.08396 [cs.HC] https://arxiv.org/abs/2212.08396

[10] Blagovesta Kostova, Seda Gürses, and Carmela Troncoso. 2020. Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy ByDesign. arXiv:2007.08613 [cs.SE] https://arxiv.org/abs/2007.08613

[11] Valentin Langholf and Uta Wilkens. 2021. Agile Project Management, New Leadership Roles and Dynamic Capabilities – Insight from a Case Study Analysis. *Journal of Competences, Strategy Management* 11 (2021), 1–18. https://doi.org/10.25437/jcsm-vol11-17

[12] Hao-Ping (Hank) Lee, Lan Gao, Stephanie Yang, Jodi Forlizzi, and Sauvik Das. 2024. "I Don't Know If We're Doing Good. I Don't Know If We're Doing Bad": Investigating How Practitioners Scope, Motivate, and Conduct Privacy Work When Developing AI Products. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 4873–4890. https://www.usenix.org/conference/usenixsecurity24/presentation/lee

[13] Carina Loiro, Hélio Castro, Paulo Ávila, Maria Manuela Cruz-Cunha, Goran D. Putnik, and Luís Ferreira. 2019. Agile Project Management: A Communicational Workflow Proposal. *Procedia Computer Science* 164 (2019), 485–490. https://doi.org/10.1016/j.procs.2019.12.210 CENTERIS 2019 - International Conference on ENTERprise Information Systems / ProjMAN 2019 - International Conference on Project MANagement / HCist 2019 - International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN/HCist 2019.

[14] Primadhika Marnada, Teguh Raharjo, Bob Hardian, and Adi Prasetyo. 2022. Agile project management challenge in handling scope and change: A systematic literature review. *Procedia Computer Science* 197 (2022), 290–300. https://doi.org/10.1016/j.procs.2021.12.143 Sixth Information Systems International Conference (ISICO 2021).

[15] Songezo Nkukwana and Nicky Terblanche. 2017. Between a rock and a hard place: Management and implementation teams' expectations of project managers in an agile information systems delivery environment. *South African Journal of Information Management* 19, 1 (2017), 10. https://doi.org/10.4102/sajim.v19i1.806

[16] Mariana Maia Peixoto. 2020. Privacy Requirements Engineering in Agile Software Development: a Specification Method.. In *REFSQ Workshops*, Vol. 2584.

[17] Maxwell Prybylo, Sara Haghighi, Sai Teja Peddinti, and Sepideh Ghanavati. 2024. Evaluating Privacy Perceptions, Experience, and Behavior of Software Development Teams. arXiv:2404.01283 [cs.SE] https://arxiv.org/abs/2404.01283

[18] Yogeshwar Shastri, Rashina Hoda, and Robert Amor. 2017. Understanding the Roles of the Manager in Agile Project Management. In *Proceedings of the 10th Innovations in Software Engineering Conference* (Jaipur, India) *(ISEC '17)*. Association for Computing Machinery, New York, NY, USA, 45–55. https://doi.org/10.1145/3021460.3021465

[19] Yogeshwar Shastri, Rashina Hoda, and Robert Amor. 2021. The role of the project manager in agile software development projects. *Journal of Systems and Software* 173 (2021), 110871. https://doi.org/10.1016/j.jss.2020.110871

[20] Olga Springer and Jakub Miler. 2018. The Role of a Software Product Manager in Various Business Environments. In *2018 Federated Conference on Computer Science and Information Systems (FedCSIS)*. 985–994.

[21] 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

[22] Torrey J. Wagner and Thomas C. Ford. 2020. Metrics to Meet Security Privacy Requirements with Agile Software Development Methods in a Regulated Environment. In *2020 International Conference on Computing, Networking and Communications (ICNC)*. 17–23. https://doi.org/10.1109/ICNC47757.2020.9049681

# Appendix

## .1 Pre-Screening Questionnaire

*Section 1: Basic Information.* To help us verify your eligibility for this study, we will ask you to upload your resume and provide a link to your LinkedIn profile. This information will be used solely to confirm your role as a project manager and will be kept confidential.

- **Your Preferred Name:**
- **Please provide us a link to your LinkedIn profile:**

*Section 2: About Your Team.*

- **Current Job Title:**
  - Project Manager
  - Product Manager
  - Scrum Master
  - Developer
  - Other
- **How long have you been working in a project management-related role?**
  - Less than 1 year
  - 1-3 years
  - 3-5 years
  - More than 5 years
- **How often do you participate in sprint planning or project planning meetings?**
  - Always
  - Often
  - Sometimes
  - Rarely

*Section 3: Experience with Agile Methodologies.* **Which Agile methodologies are you most familiar with? (Select all that apply)**

- Scrum
- Kanban
- Lean
- Extreme Programming (XP)
- Other (Please specify):

*Section 4: Project Challenges and Risk Management.* **How do you typically approach risk management in your projects?**

- Proactively identify risks and plan mitigation
- Address risks as they arise
- Delegate risk management to team members
- Minimal focus on risk management

*Section 5: Training and Certification.* **Do you hold any certifications related to project management (e.g., PMP, Agile Certified Practitioner)?**

- Yes
- No

**If yes, please list the certifications (Optional):**

*Section 6: Follow-Up Interview.* **Would you be interested in participating in a follow-up interview for this study?**

- Yes
- No

**If yes, please provide your email address so we can contact you to schedule the interview:**

## .2 Interview Protocol

*1. Team Roles and Responsibilities.*

- Can you describe your role within the Agile development team and how you interact with other team members?
- Are there specific tasks or issues related to user privacy that you feel fall outside your primary responsibilities? Can you give some examples?
- Who in your team typically addresses privacy-related concerns, such as compliance with GDPR or CCPA?

*2. Development Process and Decision-Making.*

- How does your team plan and prioritize non-functional tasks during the development cycle?
- Are privacy-related tasks considered non-functional in your process? How are they prioritized compared to other non-functional tasks?
- Have privacy-related considerations ever been deprioritized due to tight deadlines?

*3. Identifying and Addressing Risks.*

- What user-related risks do you consider when working on a new feature or project?
- How does your team address potential privacy risks, such as user data protection, that aren't immediately visible?
- Does your team use specific practices or tools to identify privacy risks early in the development cycle?
- Can you describe a time when a privacy-related issue emerged late in development? How was it managed?

*4. Integration of Non-Functional Requirements.*

- How do non-functional requirements like security, scalability, and maintainability fit into your development workflow?
- Does your team consider privacy a critical non-functional requirement not overlooked during development?
- What challenges do you face/ foresee when trying to integrate privacy into your Agile workflow?

*5. Opportunities for Improvement.*

- What improvements would you suggest to make your development process more effective or streamlined?
- Are there specific changes you'd recommend to make privacy considerations more integral to your Agile process?
- What additional support, tools, or resources would help your team better address privacy needs?

*6. Integration for Privacy Development.*

- How does your team typically approach user privacy-related issues during the development process?
- Can you share an example of a project where privacy concerns were addressed, and describe how they were managed?
- Who in your team usually raises privacy concerns, and how are these addressed when they arise?
- Do you feel privacy considerations are well integrated into your Agile workflow? Why or why not?

- Are there any specific practices or tools your team uses to ensure privacy compliance with regulations like GDPR or CCPA?

## Codebook

Below is the codebook for our study.

| Code (Level 1) | Code(Level 2) |
|---|---|
| Challenges to consider privacy | Assumed privacy is considered before they join the team |
| | Confusion between privacy and security |
| | Customer concerns are the highest priority |
| | Customer requirements vary |
| | Timelines and deadlines driven workflow |
| | |
| Privacy not being the main focus of development | Ambiguity on what data to collect |
| | No standard workflow to address privacy issue |
| | Other non-functional requirements more important than privacy |
| | Privacy concerns raised by other teams |
| | Privacy considered late in dev stage |
| | Privacy is abstract |
| | Privacy only considered when practical |
| | |
| Privacy practices | Balancing privacy and data collection |
| | Collect data with consent |
| | Collecting less info for faster development |
| | Collecting minimum info |
| | Dedicated security team |
| | Have privacy awareness during development |
| | Prioritize privacy risks based on severity |
| | Reenter spring for newly discovered privacy risks |
| | Think privacy as a feature |
| | |
| Privacy Responsibility Assignment | Developer know more about non-functional requirements |
| | Developers resolve privacy task |
| | DIvert privacy tasks to other team |
| | Lack of responsibility assignment within the team |
| | Not the team's responsibility |
| | PM and Dev raise privacy concern |
| | Trusting reputable third parties |
| | |
| Role Description | Both project manager and developer |
| | Product Manager |
| | |
| Suggestion for improvement | Dedicated Privacy team |
| | Having a privacy mindset during planning |
| | More Privacy focus on planning stage |
| | More Privacy training |
| | Privacy consultant or tool(AI) before dev |
| | Providing guide on what is safe to collect |
| | Undertstand privacy risks in customer's request |
| | |
| Privacy as a feature will not be deprioritized | |
| Sprint planning process | |

**Figure 1: Codebook used in the study.**