Usable Privacy: A Study of Norwegian Software Development Practices

Synne Stokkevåg Berg*, Katrien De Moor

NTNU – Norwegian University of Science and Technology, Trondheim, Norway

Abstract

Despite the increased focus on privacy and adoption of comprehensive data privacy laws such as the GDPR, there is still a notable absence of developer guidelines with a focus on making privacy usable, and the related practices and challenges are still poorly understood. In this context, the present study explores the current landscape of usable privacy within software development, using Norway as a case study. By means of an online survey, insights were gathered from a sample consisting of 128 developers, designers, security specialists, and related professionals. It addresses aspects such as the awareness of privacy guidelines, implementation practices, as well as challenges related to effectively incorporating privacy into software development processes. The results indicate that knowledge gaps, complicated terminology, and a lack of easily accessible toolkits and guidelines persist as barriers. Additionally, cultural attitudes towards privacy and competing priorities further obstruct the effective integration of privacy measures. Better insights into usable privacy practices can help close the gap between the technical, legal, and user-centric dimensions of privacy, aiming for a digital landscape that is both transparent and oriented toward user needs.

Keywords

Privacy, usability, software development, case study

1. Introduction and Motivation

The evolving digital landscape and technological advancements have transformed how people communicate, work, and live. However, this convenience comes at the cost of privacy, as every online activity creates a digital trace, increasing the risk of data breaches and misuse. Navigating and understanding complex privacy policies and settings can be challenging, often resulting in uninformed consent [1]. An underlying explanation for this is that few solutions effectively address both privacy and usability at the same time [2]. Saltarella et al.'s study [2] systematically reviews the translation of Privacy-By-Design and Privacy-By-Default principles into software requirements and their integration with Human-Centered Design. On one hand, comprehensive consumer data privacy laws have been developed to regulate the collection, use, and sharing of personal data, such as the General Data Protection Regulation (GDPR) [3]. However, these regulations often fall short in providing specific guidelines for developers, overlooking the importance of usability in privacy protection [2]. On the other hand, advancements in the field of Human-Computer Interaction (HCI) help enhance user experience (UX) through intuitive

Joint Proceedings of RCIS 2024 Workshops and Research Projects Track, May 14–17, 2024, Guimarães, Portugal

*Corresponding author.

synnestokkevag@gmail.com (S. Stokkevåg Berg); katrien.demoor@ntnu.no (K. De Moor)
0000-0002-8752-3351 (K. De Moor)

design and human-centered design processes. However, HCI experts are still not involved enough in the development process of privacy solutions [2, 4]. Therefore, despite the progress made in both the legal and the HCI domains, the convergence of privacy regulations and HCI principles remains insufficient and may lead to a significant gap in the creation of software that is both privacy-conscious and user-friendly.

Ackerman and Mainwaring's study [5] revealed varied user privacy concerns, from unauthorized information access and data misuse to discomfort with data collection. Mistrust towards companies handling personal data is also a concern [2], and Gundersen found that users often struggle with managing privacy settings, indicating a gap in the design of user-friendly privacy controls [1]. Earlier research further suggests that a holistic approach to privacy in software development can help bridge the gap between technical processes, users' expectations, and regulatory requirements, fostering a more transparent and protective digital environment [4]. Research targeting a better understanding of how contributors within software development perceive and respond to privacy-related issues can help identify the most pertinent challenges and hurdles that might prevent user-centric and privacy-preserving actions from being practiced.

This study investigates how software developers in Norway integrate user-centric privacy, addressing the gap in practice-oriented research. Using Norway as a case study is particularly interesting due to its high level of digitization, strong emphasis on privacy, and strict data protection laws. It examines professionals' awareness of usable privacy, their strategies, practices, and the obstacles to embedding privacy into development processes. Based on an overview of the related work (Section 2), we conducted an online survey targeting developers, designers, security specialists, and privacy experts (N=128), as briefly described in Section 3. Next, we present the results in Section 4. Finally, Section 5 discusses the implications of the findings and concludes the paper.

2. Background and Related Work

The European General Data Protection Regulation (GDPR) sets the framework for collecting, storing, and processing personal data, defining it as any information relating to an identifiable person [3]. This includes identifiable, anonymous, and pseudonymous data, each posing unique challenges for privacy and security. Despite the supposed anonymity, re-identifying individuals from such data is often possible, underscoring the complexity of data protection and the necessity for strict regulations [6, 7]. It is worth noting that there is a high bar for data to be considered truly anonymous under the GDPR [3]. Addressing developer misconceptions about what constitutes anonymous data is therefore crucial.

At the research side, the evolution of digital technology has significantly expanded the scope of personal data collection, leading to the era of Big Data. This paradigm shift, characterized by the vast accumulation and analysis of digital information, has profound privacy implications [6]. While Big Data presents new opportunities for business and operational improvements, it also poses substantial risks to individual privacy, underscoring the important balance between technological advancement and data protection [6, 7]. In this context, Birch et al. [7], for instance, highlighted how personal data has transitioned from mere information to a critical asset and, correspondingly, how Big Tech's economic interests may overshadow efforts to enhance privacy management. While the GDPR applies broadly (partly in response to the above developments) and demands legal basis for processing, such as consent, purpose limitation, and minimization [6], a key challenge remains, also years after GDPR's implementation, in bridging the gap between its legal requirements and their practical implementation in software. This has e.g., been ascribed to the fact that developers often lack clear guidance, with the GDPR's content being mostly legal and bureaucratic in nature [8].

In this overall context with potentially conflicting stakes, balancing user experience with privacy and security is challenging. Security and UI/UX improvements often occur after system development, treating these critical elements as add-ons [9]. This is problematic, as Yee [10] pointed to when stating that *"Security and usability elements can't be sprinkled on a product like magic pixie dust"*, emphasizing the need for their integration from the design phase to ensure intuitive and accessible privacy solutions. In this regard, Article 25 of the GDPR, entitled "Data protection by design and by default," more specifically emphasizes the need for early integration of privacy into the design and operation of information systems, promoting a proactive and user-centric approach to privacy [3]. It highlights the concept of "Privacy by Design", which focuses on privacy protection throughout the development process, and "Privacy by Default", which ensures minimal personal data processing [3]. However, despite the inclusion of these principles , challenges related to their practical implementation persist, often due to the GDPR's abstract nature [4].

Yet, various efforts have been made to operationalize the above principles, notably by Ann Cavoukian's "Privacy by Design"-framework [11], which outlines seven core principles for embedding privacy into system design from the start [2]. Additionally, Hoepman's "Privacy Design Strategies" provide IT developers with concrete guidelines for integrating privacy into their projects [12]. In 2017, the Norwegian Data Protection Authority issued guidelines to help organizations comply with the GDPR's Article 25 [13]. These guidelines outline a seven-step process for embedding data protection in development, from training developers in data protection to maintenance, including incident response and updates [13]. However, there's a noted lack of emphasis on usability and uncertainty regarding developers' awareness of these frameworks. Furthermore, recent studies indicated that translating the key principles into practical software development requirements remains challenging [8, 2, 14]. Software engineers may disregard methodologies that do not align with standard software practices, facing limitations in privacy solutions and a lack of systematic feedback guidelines [14]. Despite various technical solutions for regulatory compliance, more work is needed to enhance user experience [2] and to make privacy usable for all.

The underlying idea of "usable privacy" is to ensure that privacy settings are accessible to all users, regardless of technical expertise. Usable systems enable users to manage their privacy without understanding the system's inner workings [15]. The significance of usable privacy in ensuring settings and policies are manageable by all is underlined, with Wong and Mulligan noting usability's positive impact on satisfaction and policy adherence, while also warning against the risks of overlooking usability [4]. However, a complicating factor in realizing major advancements in this respect is also the fragmentation of privacy responsibility across sectors and roles, with Wong and Mulligan [4] noting that these responsibilities get fragmented among technology design, law, and social norms, preventing any single entity from fully ensuring usable privacy. They mention that while many companies have skilled UX designers/HCI experts, the latter are not always engaged in privacy efforts [4, 2]. Differences in privacy perspectives between designers and developers lead to varied implementation approaches [8].

The usability of privacy is further compromised by developers' inadequate privacy knowledge, as detailed by Saltarella et al., emphasizing the challenge of comprehending privacy's legal and technical dimensions [2]. Wong and Mulligan also note a potential gap in designers' knowledge about security and privacy [4]. The integration of HCI into privacy efforts is challenged by the need for stakeholders to understand system functionalities and legal implications comprehensively [2]. Saltarella et al., in this regard, point to the need for methodologies that blend privacy with HCI to satisfy user preferences and legal requirements. They also highlight the difficulty in translating user-focused frameworks into practical applications and the importance of developing clear, user-centric guidelines [2]. The potential under-utilization of HCI-skilled professionals in privacy projects further underlines the need to improve collaboration between designers and developers with differing privacy views and to address developers' privacy knowledge gaps through specialized education and training [2, 8].

In summary, various challenges have already been identified in the literature, however, empirical data supporting the above observations and assumptions and hypotheses they trigger, is still sparse. There is still a large need for better insights into the current practices, strategies, and the barriers and challenges at hand. Moreover, to the best of our knowledge, no studies have explicitly investigated the practices around usable privacy in the Norwegian context. Addressing the above knowledge gaps is, therefore, essential for defining concrete measures toward the successful integration of usable privacy initiatives.

3. Methodology

3.1. Survey design and implementation

A comprehensive approach is needed to explore the multifaceted perspectives, strategies, and barriers involved in integrating usable privacy into software. While the overall project underlying this work is based on a mixed-method methodology that also includes semi-structured interviews, the findings presented in this paper are based on an online survey study that was conducted. Online surveys facilitate efficient data gathering to address a specific research question, in this case privacy practices, attitudes, strategies and concerns of professionals within the Norwegian software development landscape. The survey was administered in "Nettskjema", a secure, privacy-preserving data collection tool in Norway [16]. The survey aimed to blend insights from literature with personal experiences in the IT industry, drawing from academic and professional backgrounds in security, development, and design. The survey was structured as follows: (1) personal questions to identify the respondents, (2) a series of statements to map the general attitudes and experiences of the respondents, before asking more specific questions regarding (3) awareness and understanding of privacy, (4) being updated on privacy regulations, (5) organizational practices, collaboration and integration of privacy in the development process, (6) challenges of implementing usable privacy, (7) current solutions, and (8) future directions. The survey was pre-tested with software developers pre-launch (February 2024).

3.2. Sample description and recruitment

Targeting a diverse audience within the software development lifecycle, from developers to legal advisors, was essential for gathering comprehensive insights. The distribution strategy involved direct contacts, social media platforms like LinkedIn, and specialized groups such as Slack channels for security champions, maximizing reach and diversity in responses. This multifaceted approach facilitated broad participation and enriched the study with varied perspectives on integrating privacy into software development.

In total, 128 professionals from the Norwegian software development landscape with different backgrounds and professional experiences participated. In terms of gender, 75% of the participants identify as male, 23% as female, and 2% preferred not to say. The average age is 36 (S.D. 10.32), and 68.8% of the respondents are in the age group of 25-44. In terms of education, 28% of the participants hold a bachelor's degree, and 66% a master's or higher.

IT consultancy firms are the most represented organization type (59%), followed by in-house IT firms (23%), and IT startups (6%). Regarding further employment characteristics, 62% works in the private sector and 38% in the public sector. The employment sectors represented are also diverse, including 16% in healthcare and welfare, 13% in media and entertainment, and 12% in energy and oil, among others. Participants further differ in their roles within their companies, with 58% serving as software developers, 13% as security specialists, and 8% as designers, among other positions. Respondents' experience levels within software development vary widely, from up to 2 years (14%), 2-4 years (31%), 5 to 10 years (13%), 10 to 19 years (20%), and more than 19 years of experience (22%), hence assuring that diverse perspectives were captured.

4. Results

Awareness and understanding. First, we consider the respondents' *awareness and understanding of privacy*, as visualized in Figure 1. In this respect, nearly 7 out of 10 respondents *agreed* that they have a good understanding of privacy regulations related to software development. Additionally, more than half of the respondents *agreed* that they are aware of the challenges associated with integrating usable privacy.

Organizational practices and collaboration. When it comes to *organizational practices and collaboration*, only 54% *agreed* that different roles in their organization collaborate effectively to address privacy issues. Further, less than one-third of the respondents indicated that they are provided with adequate organizational support for integrating privacy in software development (Figure 1), and 1 out of 2 respondents *disagreed* that there are uniform privacy approaches across teams and clearly defined responsibilities concerning usable privacy within their organization.

Integration of privacy in the development process. As illustrated in Figure 1, more than 1 out of 2 respondents *agreed* that their team's privacy efforts meet only minimal requirements. Privacy concerns being prioritized and addressed early in the development cycle yielded more mixed opinions: 38% *agreed*, and 38% *disagreed.* Finally, when asked about *challenges of implementing usable privacy*, 52% indicated facing challenges in implementing usable privacy, and 56% agreed that privacy often conflicts with usability/UX goals.

Design frameworks and compliance with guidelines. Among those respondents who utilize design frameworks (representing 52% of the respondents), only 23% acknowledge the incorporation of privacy considerations into these methodologies. Others are unsure (39%) or indicated that privacy is not integrated and evaluated in these design processes (38%). Regarding the guidelines developed by the Norwegian Data Protection Authority, 38% reported familiarity with the guidelines but hadn't read them, while only 23% reported having read and occasionally or regularly used them in their work.

Main barriers. Figure 2 shows the responses regarding the *main barriers* to implementing usable privacy in software as reported by practitioners. The findings indicate that insufficient knowledge constitutes a significant obstacle, identified by more than half of the respondents. Additionally, both challenges of balancing privacy concerns with other requirements and budget constraints were highlighted by around 4 out of 10 participants. Additional barriers highlighted in an open question included: complicated terminology, leaving much of the implementation to individual interpretation, overly specific regulations hindering UX, poor collaboration between lawyers and designers, minimal consequences for non-compliance, insufficient support tools for privacy by design in agile environments, complex regulations leading to user click-fatigue, and conflicting customer interests.

Training or resources. *Training or resources* to enhance usable privacy can play an important role in this respect. Figure 2 shows the practitioners' preferences: nearly 6 out of 10 prefer technical guides and toolkits for developing and testing privacy features. Further, nearly half of the respondents want hands-on workshops on privacy integration, and 4 out of 10 want collaboration with privacy experts or legal advisors for legal insights.

Additional feedback. In the survey's open-ended section, many respondents provided additional comments. Here, one respondent suggested that the dichotomy between user experience and privacy is false and that both can be harmoniously integrated. In addition, cultural issues, including a systemic disregard for privacy in software development, were mentioned to contribute to viewing privacy as peripheral. Further, it was put forward that challenges in prioritizing privacy in client projects, especially startups, arise due to a focus on legal minimums over substantial privacy considerations. Overall, several respondents also called for more practical resources, such as case studies and pattern descriptions, and accessible templates or checklists from regulatory entities (such as the Norwegian Data Protection Authority) to aid development. Finally, a lack of leadership support for user-friendly privacy options was noted, stemming from misconceptions about data collection limitations and cost implications.

5. Discussion and Conclusion

In this study, we investigated the current practices around usable privacy in Norwegian software development, focusing on uncovering practitioners (N=128) attitudes, practices, and encountered challenges. Although a significant percentage of participants (68%) believe that they understand privacy regulations well, this self-reported proficiency appears to contrast with prior studies , which shows a general lack of privacy knowledge among developers [8, 2, 4]. This discrepancy suggests that developers might overestimate their understanding of privacy laws. Interestingly, "a limited understanding of privacy" was identified as a major barrier to implementing effective privacy measures, indicating a gap in privacy education and a potential area for future research and tailored measures.

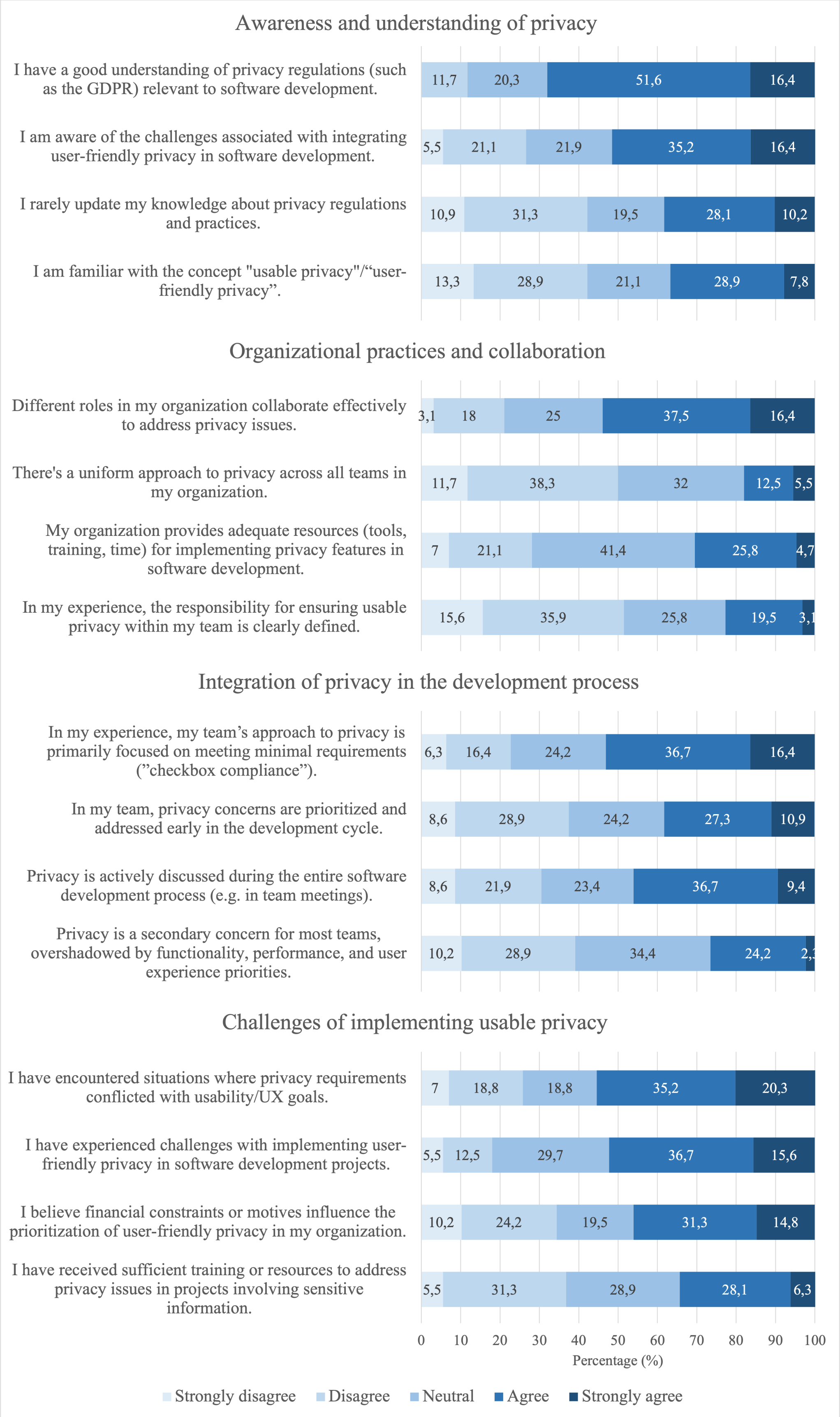

Figure 1: Self-reported attitudes and experiences (percentages, N=128).

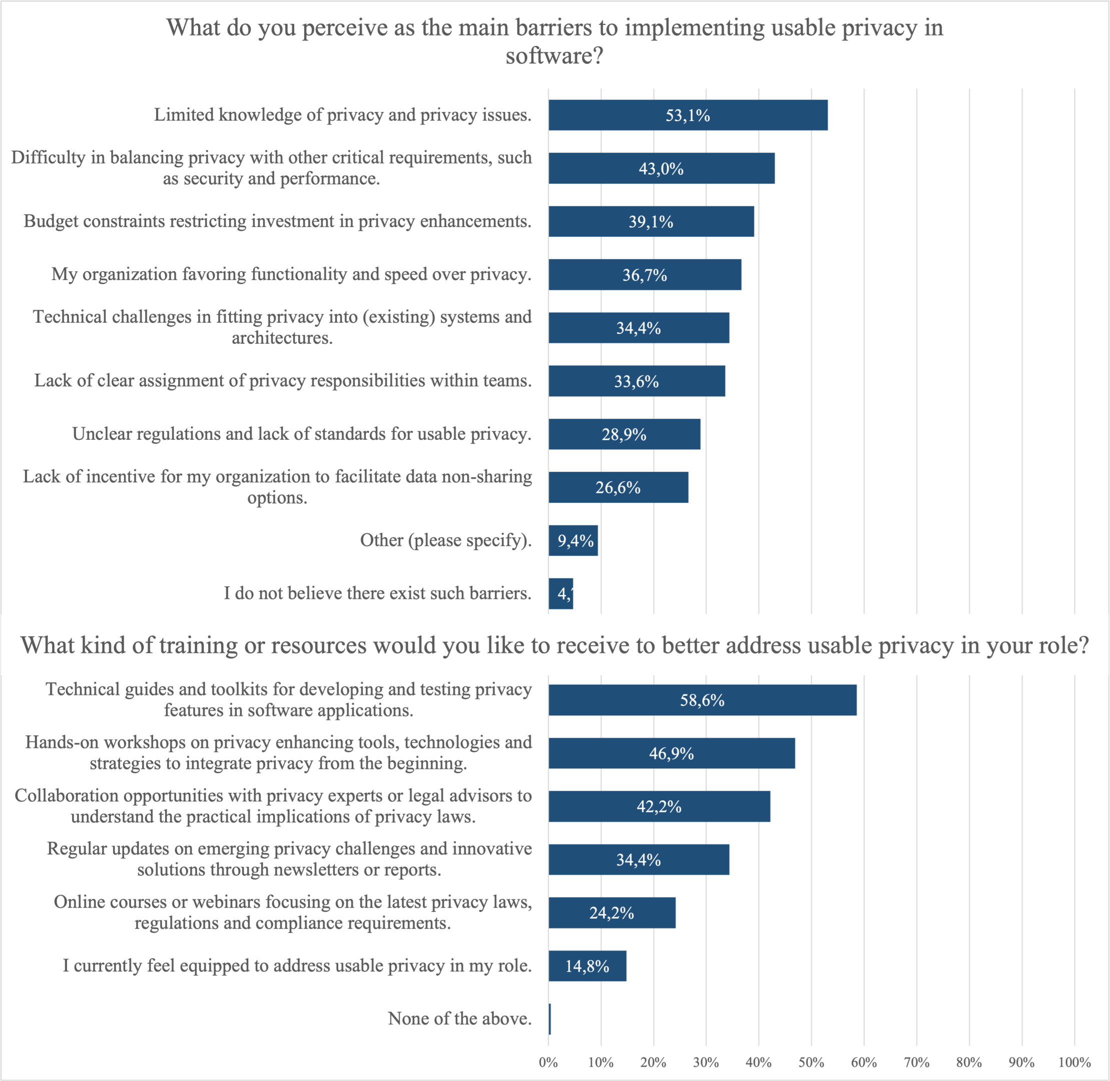

Figure 2: Main barriers and resources to improving usable privacy (percentages, N=128).

The findings also reveal that respondents are aware of (52%) and have experienced (52%) challenges in applying privacy in practice, suggesting a gap between knowledge about privacy principles and the ability to apply them effectively. Additionally, many respondents agreed that their team's approach to privacy is primarily focused on meeting minimal requirements, underscoring compliance-first mindsets rather than comprehensive privacy strategies (see Figure 1). The preference for "Technical guides and toolkits" (59%) highlights the need for practical tools to help integrate privacy into development work, such as case studies, pattern descriptions, and easily accessible templates or checklists from regulatory bodies (such as the Norwegian Data Protection Authority). Implicitly, the findings also illustrate the gap between academic research and actual real-world practice when it comes to usable privacy.

The data from Figure 2 further highlight the key challenges in implementing usable privacy in Norway, with insufficient knowledge marked as a significant barrier by many respondents. This issue, alongside balancing privacy with other demands and budget limits, points to the complex hurdles in privacy-centric software development. Interest in workshops and expert collaboration suggests a desire for experiential learning and deeper legal understanding. In line with [2], additional barriers such as unclear terminology and regulatory challenges stress the need for better education. Through the open-ended responses, it was also suggested that the culture around privacy plays an important role, next to knowledge, tools and skills. This perspective, particularly prevalent in client projects and startups, may lead to challenges in prioritizing comprehensive privacy considerations, with a tendency to focus on meeting legal minimums rather than embedding substantive privacy measures.

Overall, this study illustrated the nuanced challenges and perceptions surrounding privacy within Norwegian software development. It underscores the existence of knowledge gaps. Despite developers' awareness of privacy challenges, there seems to be a notable gap in applying privacy principles effectively, driven by a compliance-first mindset rather than a holistic approach to privacy. The demand for practical tools, such as technical guides and workshops, underscores the need for improved privacy education and resources to bridge the gap between theoretical knowledge and its practical application. Addressing these needs is crucial for enhancing usable privacy in software development.

In future work, we plan to analyze the potential differences between professional roles, companies, and domains, as well as conduct in-depth interviews to deepen the insights from the survey. Additionally, follow-up work should consider a larger sample, include other countries and diverse perspectives, and explore which tools, strategies, and collaborative efforts can contribute to the creation of both regulatory-compliant and user-friendly privacy solutions *in practice*.

References

[1] I. Gundersen, Privacy Management and Preservation in the Era of Targeted Advertising, Master's thesis, Norwegian University of Science and Technology, 2022. URL: https://hdl.handle.net/11250/3026224.

[2] M. Saltarella, G. Desolda, R. Lanzilotti, V. S. Barletta, Translating privacy design principles into human-centered software lifecycle: A literature review, International Journal of Human-Computer Interaction (2023). doi:10.1080/10447318.2023.2219964.

[3] EU regulation 2016/679 (General Data Protection Regulation) on personal data protection, 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[4] R. Y. Wong, D. K. Mulligan, Bringing design to the privacy table broadening "design" in "privacy by design" through the lens of HCI, in: ACM Conference on Human Factors in Computing Systems, 2019. doi:10.1145/3290605.3300492.

[5] M. S. Ackerman, S. D. Mainwaring, Privacy issues and human-computer interaction, 2008. URL: https://api.semanticscholar.org/CorpusID:14493572.

[6] N. Gruschka, V. Mavroeidis, K. Vishi, M. Jensen, Privacy issues and data protection in big

data: A case study analysis under gdpr, in: 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 5027–5033. doi:10.1109/BigData.2018.8622621.

[7] K. Birch, D. Cochrane, C. Ward, Data as asset? the measurement, governance, and valuation of digital personal data by big tech, Big Data & Society 8 (2021). doi:10.1177/20539517211017308.

[8] V. Barletta, G. Desolda, D. Gigante, R. Lanzilotti, M. Saltarella, From GDPR to privacy design patterns: The MATERIALIST framework (2022) 642–648. doi:10.5220/0011305900003283.

[9] M. Alshamari, A review of gaps between usability and security/privacy, International Journal of Communications, Network and System Sciences 9 (2016) 413–429.

[10] K.-P. Yee, Aligning security and usability, IEEE Security & Privacy 2 (2004) 48–55. doi:10.1109/MSP.2004.64.

[11] A. Cavoukian, Privacy by design: the 7 foundational principles, Information and privacy commissioner of Ontario, Canada 5 (2009) 12.

[12] J.-H. Hoepman, Privacy Design Strategies (The Little Blue Book), Nijmegen : Radboud University, 2018. URL: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.

[13] Norwegian Data Protection Authority, Software development with data protection by design and by default, 2017. URL: https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/.

[14] J. C. Caiza, Y.-S. Martín, D. S. Guamán, J. M. Del Alamo, J. C. Yelmo, Reusable elements for the systematic design of privacy-friendly information systems: A mapping study, IEEE Access 7 (2019) 66512–66535. doi:10.1109/ACCESS.2019.2918003.

[15] A. Pattakou, A.-G. Mavroeidi, V. Diamantopoulou, C. Kalloniatis, S. Gritzalis, Towards the design of usable privacy by design methodologies, in: 2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE), 2018, pp. 1–8. doi:10.1109/ESPRE.2018.00007.

[16] Nettskjema's website, 2024. URL: https://nettskjema.no/.