Securing Engagement: Key Takeaways from Onboarding Users into Data Protection Apps

Lennart Kiss [1], Rachelle Sellung [2]

Abstract: This paper examines persistent challenges users/citizens face in exercising their data protection rights under the General Data Protection Regulation (GDPR), particularly in everyday digital contexts. It presents findings from the BMBF-funded Tester project, which developed a privacy assistant to support transparency, intervenability, and data protection literacy in the context of self-tracking and health-monitoring devices. Focusing on the onboarding experience, this study explores how users engage with a GDPR-aligned privacy assistant through an iterative, human-centered design process. Based on mixed-method user evaluations, we validate key usability strategies—such as personalization, grouped customization, and adaptive content—that can promote awareness and improve informed user decision making. The results offer lessons for the design of onboarding experiences in privacy-focused applications and contribute to broader efforts to make digital privacy rights more accessible, transparent, and usable.

Keywords: Privacy Assistant, Usability, User Experience, GDPR, Data Protection, Privacy

1 Introduction

The General Data Protection Regulation (GDPR), introduced in 2018, grants individuals the right to control their personal data. However, practical implementation of these rights remains challenging for many users [GML20, ZMM24]. Transparency around data processing and effective mechanisms for intervenability are still limited, particularly in consumer-facing applications that handle sensitive personal data. While the legal framework is well defined, its usability in everyday contexts often falls short [JF20]. This paper addresses those challenges through the lens of onboarding in data protection applications. For simplicity, the onboarding process is generally defined as the "sequence of steps that introduces users to a new product or service" [Ca17]. In our case specifically in the context of a privacy assistant for users of self-tracking and health-monitoring devices developed within the Tester Project funded by the German federal ministry for education and research (BMBF). These third-party self-measurement devices, often used for fitness or chronic disease management, collect large volumes of personal and sensitive data. Yet users frequently remain unaware of what data is

[1] University of Stuttgart, Institute of Human Factors and Technology Management (IAT), Identitymanagement, Allmandring 35, Stuttgart, 70569, lennart.kiss@iat.uni-stuttgart.de https://orcid.org/0009-0000-8839-5470
[2] Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering IAO, Identitymanagement, Nobelstrasse 12, Stuttgart, 70569, rachelle.sellung@iao.fraunhofer.de https://orcid.org/0000-0003-1235-030X

doi:10.18420/OID2025_10

collected, how it is processed, and by whom. Traditional onboarding flows in consumer applications focus on basic feature introductions or account setup to convert first time users into long term users [Ca22, SF23]. In contrast, onboarding in privacy-focused tools must also serve as a critical educational and trust-building function. The onboarding process studied in this work aimed to introduce a GDPR-aligned privacy assistant for improving transparency and user control over self-tracking data. The assistant includes features such as a dashboard to show data flows, a help desk for exercising GDPR rights, and an information center with educational materials tailored to the user's data protection literacy. Therefore, the onboarding was designed to build a user's understanding of relevant data flows and to prepare them to make informed decisions about their data processing events later in the application experience. The contribution of this paper is twofold. First, it presents an empirical evaluation of how users engage with privacy-related onboarding in a real use case based on qualitative study data. Second, it identifies design strategies that support user empowerment through transparency, especially in data ecosystems where users have low visibility and high dependency on third-party device ecosystems. The rest of the paper is structured as follows: Section two reviews related work on user experience in privacy assistants and onboarding. Section three outlines the design and evaluation methodology. Section four presents key findings from user studies. Section five discusses the implications for privacy tool design. Section six reflects limitations and future research, and Section seven concludes with a summary.

2 Related Literature

This chapter outlines related research on three relevant topics to this work. First, this section will explore the literature on the user experience perspective of Data Protection, in particular related to GDPR. Next, it will summarize related research on privacy assistants. Lastly, there is a brief overview of the topic of user experience in onboarding.

Despite its legal clarity, the GDPR offers limited guidance on how to implement user rights in a usable way. [JF20] highlight the lack of concrete implementation guidance for usability in data protection systems. Additionally, [AM21] report that UX designers often rely on informal practices when addressing GDPR compliance with no long-term sustainability, indicating a need for structured methodologies. Privacy preferences are often highly subjective and context-dependent, varying by data type and retention period [AJL13, Em21]. This complexity underscores the challenge of creating understandable interfaces for privacy control. Studies also show that users struggle with the length and legal complexity of privacy policies [Eb21, Ac16, WZH17], with estimates suggesting it would take hundreds of hours annually to read them thoroughly [Gl16]. There have been attempts to improve privacy policies in how they are visualized for users [ST20, CMU25, CGA06]. Recent research into privacy assistants explores how digital tools can support users in managing personal data, particularly in contexts like the Internet of Things (IoT) [AZ19, Da18] and mobile apps [Li16]. However, many of these tools are developed without sufficient user involvement or attention to human-centered interface

design [St23]. Furthermore, [St23] emphasizes the need for privacy assistants to support key functions such as privacy configuration, awareness building, and motivation, and found that users expect both automation within settings configuration as well as alerts about potential privacy threats. Onboarding has been studied extensively in general UX literature [Ca03, SGV18], but much less in the context of privacy and data protection. [Ga19] outlines three key components of effective onboarding—UI patterns, contextual educational content, and contextual communication. The Minimalist Instruction framework by [Ca14] advocates for action-oriented, error-resilient onboarding flows. [SF23] presents a larger summary of his work. However, this identifies similar themes of engagement and learning presented in [Ga19]. Additionally, privacy onboarding differs from commercial onboarding in that its goal is not just immediate feature engagement, but long-term user empowerment, trust, and informed control over personal data.

3 Methodology

This study applied a design science approach in accordance with [He04] to develop and evaluate a privacy assistant focused on onboarding users in the context of self-tracking and health-monitoring devices. The objective was to design an onboarding process that supports transparency and user empowerment under the GDPR, particularly in complex, third-party device ecosystems. The methodology followed an iterative cycle of design, evaluation, and refinement. The initial prototype was based on prior user research within the project on user needs, self-tracking behaviors, and expectations regarding transparency and intervenability [Fl22, Fl24]. The resulting onboarding process was then refined through multiple rounds of expert reviews and user testing.

The onboarding flow was structured around five sequential steps, each designed to reduce cognitive burden and progressively increase user awareness of personal data flows. It begins with a brief, non-technical introduction that communicates the assistant's purpose and benefits, setting the stage for what users can expect. This is followed by an account setup phase or an optional guest mode for anonymous exploration. Subsequently, users are guided through a device selection process, where they connect their self-tracking devices. This step provides the assistant with the necessary context to inform users about what data is being collected and by which devices. Next, users configure their privacy preferences by selecting one of three pre-configured privacy profiles—ranging from restrictive to permissive—with the option to manually adjust settings if desired. The final step asks users to self-assess their familiarity with data protection concepts. Based on this input, the assistant tailors the tone and depth of educational content offered within the app. Importantly, all steps in the onboarding flow are optional and skippable, allowing users to engage at their own pace.

The first development stage of the privacy assistant was assessed by means of expert reviews. Subsequently in the following stages user testing was conducted in two iterations, involving a total of 26 unique participants. Due to logistical constraints, the

same sample could not be retained across both sessions. To ensure consistency in participant profiles, each participant was asked to identify with one of the predefined personas established earlier in the project [Fl24]. Quantitative evaluation employed the System Usability Scale (SUS) to measure perceived usability, the User Experience Questionnaire (UEQ) to assess both hedonic and pragmatic aspects of the interaction, and A/B testing to compare variations in transparency and intervenability features. Qualitative data were gathered through post-task and post-test questionnaires. Key coding dimensions included usability factors such as user-friendliness, interface clarity, terminology, and error comprehension; user expectations; consistency and aesthetics of design; and accessibility. Additionally, the analysis addressed data protection attitudes. Error analysis covered both the source and severity of errors. Reflections captured exclusively in the post-test phase included overall satisfaction, engagement patterns, perceived usage barriers, comparisons to similar tools, and perspectives on the assistant's impact on transparency and intervenability.

4 Findings and Lessons Learned

This section summarizes the outcomes of user testing conducted across three development iterations of the privacy assistant's onboarding process. The qualitative findings reflect recurring themes in usability, user engagement, and comprehension. They are grouped by strengths, identified challenges, and design lessons that emerged during the iterative process.

Overall, users responded positively to the onboarding experience. The introductory screen effectively communicated the assistant's purpose without overwhelming users. Participants appreciated the clean interface, visual aids, and flexible design, including the ability to skip steps or enter via a guest mode. The account setup process was perceived as intuitive, with clear guidance for actions. Feedback mechanisms—such as progress indicators and confirmation screens—were frequently cited as helpful in structuring the process and motivating users to continue. These design elements contributed to a sense of clarity and control during onboarding and reflect the effectiveness of the design principles discussed in the related literature. Despite the generally positive reception, several challenges were observed in later onboarding steps. While connecting self-measurement devices was straightforward, the purpose and implications of privacy preference configuration were often unclear. Users struggled to understand how their selections would affect the app's future behavior. This gap suggests a need for more explicit communication of how these settings influence the assistant's reports and recommendations. Participants also reported difficulty differentiating between the pre-configured privacy profiles. Some chose at random or based on assumed "safety," without a clear understanding of the trade-offs. Although manual configuration was available, it was rarely used due to perceived complexity. The adaptive educational content, which adjusted based on users' self-assessed privacy knowledge, was well received. However, some users expected this adaptability to extend

beyond the Information Center into other parts of the app, resulting in mismatched expectations. The following insights summarize design strategies that improved onboarding effectiveness and highlight areas for future enhancement:

- **Personalization must be tied to Tangible Outcomes:** Users valued adaptive features but needed clear, real-time feedback connecting their choices to meaningful results. Visual previews or usage scenarios could improve comprehension.
- **Iterative Refinement is Non-Negotiable:** Repeated testing revealed subtle but significant usability barriers that were not evident in initial expert reviews. Frequent feedback loops ensured alignment with user expectations and interaction patterns.
- **Adaptive Content should anticipate User Expectations:** Users should be informed about which parts of the system are personalized. Without this clarity, adaptive features risk generating confusion rather than empowerment.
- **Feedback Mechanisms are integral to Engagement:** Features like progress bars and confirmation screens are not cosmetic—users consistently cited them as motivational and informative. They should be considered essential components in onboarding design.
- **Simplified Complexity through Grouped Customization:** To reduce cognitive load, future iterations should organize privacy preferences by themes or data types. This would help users engage more confidently without requiring expert-level understanding.

5 Discussion

This study contributes to ongoing efforts to improve data protection by examining how onboarding can support user empowerment in privacy-focused applications. Through empirical evaluation of a privacy assistant designed for users of self-tracking devices, this work identifies actionable design strategies that address key usability barriers while maintaining relevance to GDPR principles of transparency and intervenability. In the context of data protection, onboarding becomes a strategic point of engagement: it sets the foundation for user understanding of complex data flows and initiates a mental model for managing privacy preferences. This framing distinguishes privacy onboarding from traditional feature onboarding and underscores its domain specificity. Our work demonstrates that onboarding can be structured to increase data protection literacy without requiring immediate, high-stakes decisions. Pre-configured privacy settings and adaptive educational content, when properly explained and scoped, reduce decision fatigue while still providing control. These design elements support privacy as a process, rather than a one-time opt-in. This paper contributes to a growing but still limited body of research on human-centered privacy design. While many privacy tools aim to enforce compliance or automate protection, few address how users are introduced to these tools and the role of first-time interactions in building trust and enabling autonomy. By

focusing on onboarding, we highlight a phase in the privacy interaction lifecycle that has tangible effects on user behavior and retention. Our study also validates several design principles in a privacy-specific context. These include the importance of progressive disclosure, grouped customization, and feedback-rich interactions, which together create a more navigable and engaging onboarding process. Finally, the iterative nature of our approach demonstrates how empirical UX research can shape the development of effective privacy tools. Our mixed-methods evaluation revealed not only usability strengths and weaknesses, but also user expectations, misinterpretations, and the unintended consequences of unclear feature boundaries. These insights are critical for translating GDPR rights into usable, real-world applications.

6 Limitations and Future Work

While this study provides important insights into the onboarding of privacy-focused applications, its limitations should be acknowledged. First, the privacy assistant evaluated in this work was tested in a simulated environment, with certain features (e.g., account creation, authentication) mimicked for the purpose of usability testing. No real user data was processed or stored, and the assistant was not deployed in a live system. This limitation restricts our ability to assess how users would respond to real-world consequences of their interactions, particularly in terms of long-term trust and data protection behavior. Second, the study focused primarily on short-term usability and user experience metrics. While the findings illustrate how onboarding supports comprehension and engagement at the initial interaction stage, they do not account for retention, behavior change, or sustained use over time. Longitudinal studies would be necessary to evaluate whether the onboarding experience leads to more informed or proactive privacy management in the long run. Additionally, expanding the adaptive content model to cover more interaction layers of the application—while managing user expectations—could further enhance usability without compromising simplicity.

7 Conclusion

This paper examined how onboarding can be leveraged to support user engagement and comprehension in privacy-focused applications, specifically through the development and evaluation of a GDPR-aligned privacy assistant for self-tracking scenarios. By applying a design science approach and involving users throughout the development cycle, we identified onboarding strategies that reduce complexity, build trust, and improve early understanding of personal data flows. Our findings demonstrate that onboarding is not merely a functional prelude but a critical phase in the privacy interaction lifecycle. Design elements such as grouped customization, adaptive content, and feedback mechanisms were linked to enhanced usability while directly supporting privacy goals, including transparency and user empowerment. The scientific contribution

of this work lies in bridging the gap between legal rights and practical usability. We show how empirical, user-centered methods can produce onboarding experiences that not only lower the barrier to entry but also prepare users to act meaningfully within the constraints of today's digital environments. By focusing on securing engagement at the earliest stage of interaction, this research contributes to the design of more effective, human-centered privacy tools that support not just compliance, but comprehension, agency, transparency and intervenability.

Bibliography

[Ac16] Acquisti, A. et al.: The economics of privacy. Journal of Economic Literature, 54, pp. 442–492, 2016.

[AJL13] Acquisti, A.; John, L. K.; Loewenstein, G.: What is privacy worth? In: The Journal of Legal Studies, Bd. 42, Nr. 2, S. 249-274, 2013.

[AM21] Almeida, F.; Monteiro, J. A.: Exploring the Effects of GDPR on the User Experience. In: Journal of Information Systems Engineering and Management, Bd. 6, Nr. 3, em0140, 2021.

[AZ19] Andrade, L.; Zorzo, S.: Privacy Everywhere: A Mechanism for Decision Making and Privacy Assurance in IoT Environments. 2019.

[Ca03] Carroll, J. M.: Introduction: Toward a Multidisciplinary Science of Human-Computer Interaction. In: HCI Models, Theories, and Frameworks: Toward a Multidisciplinary Science, S. 1–9, Elsevier Inc., 2003.

[Ca14] Carroll, J.: Creating Minimalist Instruction. In: International Journal of Design for Learning, Bd. 5, Nr. 2, 2014.

[Ca17] Cascaes Cardoso, M.: The Onboarding Effect: Leveraging User Engagement and Retention in Crowdsourcing Platforms. In (ed.): Proc. 2017 CHI Conf. Ext. Abstr. on Human Factors in Comput. Syst., 2017.

[Ca22] Cascaes Cardoso, M.: User Onboarding Design in Citizen Science: A Path to Grow Engagement and Participation. PhD thesis, 2022.

[CGA06] Cranor, L. F.; Guduru, P.; Arjula, M.: User Interfaces for Privacy Agents. In: ACM Transactions on Computer-Human Interaction, Bd. 13, S. 135–178, 2006.

[CMU25] Carnegie Mellon University, www.usableprivacy.org, accessed: 30/01/2025.

[Da18] Das, A. et al.: Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. IEEE Pervasive Comput. 17, pp. 35–46, 2018.

[Eb21] Ebbers, F. et al.: User Preferences for Privacy Features in Digital Assistants. Electron. Markets 31, pp. 411–426, 2021.

[Em21] Emami-Naeini, P. et al.: Privacy Expectations and Preferences in an IoT World. In (ed.): Proc. SOUPS 2017. USENIX Association, Berkeley, CA, pp. 399–412, 2017.

[Fl22] Floris, A.: Who is the self-tracker? Establishing an initial instrument to holistically

assess self-tracking behaviours. Master's thesis, University of Twente, 2022.

[Fl24] Floris, A.; Astfalk, S.; Sellung, R.; Roßnagel, H.: Tracking or being tracked: How much do self-trackers care about their data's privacy? In (ed.): Sicherheit 2024. Gesellschaft für Informatik e.V., pp. 121-136, 2024.

[Ga19] Galavan, R.: C.A.R.E. – A Simple Customer Onboarding Framework. In: Intercom Onboarding, S. 20–28, 2019.

[Gl16] Gluck, J. et al.: How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. In (ed.): Proc. 12th USENIX Conf. on Usable Privacy and Security (SOUPS '16). USENIX Association, Berkeley, CA, pp. 321–340, 2016.

[He04] Hevner, A. R. et al.: Design Science in Information Systems Research. In: MIS Quarterly, Bd. 28, Nr. 1, S. 75–105, 2004.

[JF20] Johansen, J.; Fischer-Hübner, S.: Making GDPR Usable: A Model to Support Usability Evaluations of Privacy. In (ed.): Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology, Volume 576, Springer, Cham, 2020.

[Li16] Liu, B. et al.: Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In (ed.): Proceedings of the 12th USENIX Conference on Usable Privacy and Security (SOUPS '16). USENIX Association, Berkeley, CA, pp. 27–41, 2016.

[SF23] Svanström, N.; Fredriksson, A.: User Onboarding Experience – Increasing Users' Perceived Motivation of Engaging More with a Product. Master's thesis, Chalmers University of Technology, 2023.

[SGV18] Strahm, B.; Gray, C. M.; Vorvoreanu, M.: Generating Mobile Application Onboarding Insights Through Minimalist Instruction. In: Proceedings of the 2018 Designing Interactive Systems Conference, S. 361–372, 2018.

[ST20] Soumelidou, A.; Tsohou, A.: Effects of Privacy Policy Visualization on Users' Information Privacy Awareness Level. Information Technology & People 33, pp. 502–534, 2020.

[St23] Stöver, A. et al.: Investigating How Users Imagine Their Personal Privacy Assistant. Proceedings on Privacy Enhancing Technologies Symposium 2023/2, pp. 384–402, 2023.

[WZH17] Mihale-Wilson, C.; Zibuschka, J.; Hinz, O.: About User Preferences and Willingness to Pay for a Secure and Privacy-Protective Ubiquitous Personal Assistant. In (ed.): Proc. 25th European Conf. on Information Systems (ECIS), Guimarães, Portugal, pp. 32–47, 2017.

[ZMM24] Zaguir, N. A.; de Magalhães, G. H.; de Mesquita Spinola, M.: Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions. IEEE Access 12, pp. 81608–81630, 2024.