Data Privacy in Software Practice: Brazilian Developers' Perspectives – Extended Abstract – CTDG-SI 2026

Aryely Matos[1], **Anderson Uchôa (Supervisor)**[1],
Juliana Alves Pereira (Co-supervisor)[2]

[1] Federal University of Ceará (UFC)
Itapajé – CE – Brazil

[2]Pontifical Catholic University of Rio de Janeiro (PUC-Rio)
Rio de Janeiro – RJ – Brazil

aryelymatos@alu.ufc.br, andersonuchoa@ufc.br, jpereira@inf.puc-rio.br

Abstract. *This extended abstract presents a study on data privacy in software development practice. Based on a survey with 88 Brazilian developers with privacy-related experience, it investigates their awareness of data privacy, perceptions of privacy strategies, and the influence of organizational factors. Our results reveal gaps between developers with direct and indirect privacy experience. While strategies such as encryption are widely adopted and perceived as highly important, others, such as disabling data collection, show that ease of use does not necessarily lead to adoption. We also found that the absence of dedicated privacy teams is associated with lower prioritization and reduced investment in tools. Overall, the findings highlight the role of organizational context in shaping privacy practices and provide insights to improve privacy engineering in software development.*

1. Introduction

The increasing complexity of software systems and the rapid evolution of data protection regulations, such as GDPR and LGPD, have made data privacy a central concern in software engineering [Kempe and Massey 2021]. Developers must align their practices with regulatory demands; however, achieving compliance remains challenging due to the inherent complexity of these regulations, overlapping requirements, and the difficulty of translating legal constraints into actionable engineering practices [Kempe and Massey 2021, Canedo et al. 2023, Iwaya et al. 2023].

Despite its growing importance, translating data privacy requirements into practice remains challenging. Prior work has explored privacy requirements elicitation and structuring [Canedo et al. 2023], developers' perceptions and practices [Iwaya et al. 2023], and organizational influences such as privacy champions [Tahaei et al. 2021]. However, these studies offer only a partial view, often addressing these aspects in isolation. There is limited empirical evidence on how developers jointly reason about privacy, assess strategies, and integrate them into workflows. In particular, it remains unclear how perception dimensions, such as *importance*, *ease of use*, and *frequency*, interact across developer profiles and organizational contexts. This gap limits understanding of why important practices are not consistently adopted, hindering their effective operationalization.

This paper presents an extended abstract of a prior study [Matos et al. 2025] based on a survey with 88 Brazilian developers with privacy-related experience. We provide a

multi-dimensional empirical analysis of how developers understand, evaluate, and apply data privacy practices in real-world settings. Our contributions are threefold. First, we quantify developers' awareness of data privacy using a structured set of 21 statements spanning knowledge, attitudes, and behaviors (RQ_1). Second, we systematically analyze the relationships between perceived importance, ease of use, and actual adoption of privacy strategies, revealing misalignments that indicate practical integration challenges (RQ_2). Third, we investigate how organizational factors – particularly the presence of dedicated privacy roles and teams – influence the prioritization and adoption of privacy practices (RQ_3). By providing an integrated view of awareness, perception, and organizational influence, this study contributes to bridging the gap between regulatory expectations and the practical adoption of data privacy in software development.

2. Study Settings

We conducted a survey comprising 35 questions, including 21 statements grounded in the Knowledge-Attitude-Behaviour (KAB) model [Schrader and Lawless 2004] and evaluated on a 5-point Likert scale. Using a snowball sampling strategy, the survey was disseminated via social media platforms and remained open for 132 days. In total, we collected 122 responses, of which 88 were retained after excluding participants with no direct or indirect experience in data privacy. For the analysis, we stratified participants based on key factors, including *direct vs. indirect privacy experience*, *specialist vs. non-specialist* roles, and *organization size*. After, we analyzed 13 data privacy strategies (e.g., encryption, anonymization, and data minimization), considering three dimensions: *frequency of use*, *perceived importance*, and *ease of use*. We applied a weighting and normalization approach, and conducted statistical tests (Wilcoxon Rank Sum [Whitley and Ball 2002] and Cliff's Delta [Grissom and Kim 2005]) for group comparisons, complemented by Grounded Theory procedures [Corbin and Strauss 2008] for open-ended responses[1].

3. Main Takeaways

RQ_1 – Awareness of Data Privacy. Overall, developers exhibit a high awareness of data privacy concepts, frequently associating privacy with security (e.g., 33 mentions as the first term). However, this awareness varies significantly across groups. Participants with direct privacy experience (61.4%, 54/88), specialists, and those in larger organizations report higher awareness levels, with statistically significant differences observed in 12 out of 21 statements ($p < 0.05$). For instance, developers with direct experience show higher agreement in proactive behaviors such as proposing solutions (mean = 4.19 vs. 3.76). These results indicate that awareness is not homogeneous, but shaped by experience, role, and organizational context. **RQ_2 – Perception of Privacy Strategies.** We observe a clear misalignment between perceived importance, ease of use, and actual adoption of privacy strategies. While strategies such as encryption achieve very high perceived importance ($\approx$ 94%) and are widely adopted, others – such as turning off data collection – remain underutilized despite moderate-to-high importance. This discrepancy confirms that perceived value alone does not drive adoption and highlights the role of practical and organizational constraints. **RQ_3 – Organizational Influence.** Organizational factors emerge as critical drivers of privacy adoption. Participants from larger organizations (e.g., 43.1% in companies with >1000 employees) report higher engagement in privacy training ($p = 0.01$) and

[1]Further details are in our replication package: https://doi.org/10.5281/zenodo.14345392

stronger knowledge of privacy practices ($p = 0.02$). The presence of dedicated privacy teams and tools is consistently associated with higher prioritization and adoption, whereas their absence leads to fragmented practices. These findings reinforce that effective privacy adoption depends on both individual awareness and organizational support.

4. Conclusions and Future Work

This study highlights that although developers recognize the importance of data privacy, their awareness of regulations such as the GDPR and LDPD remains uneven and limited. More critically, we uncover a consistent misalignment between perceived importance and actual adoption: while strategies such as *Encryption* and *User Control* are widely used, others, such as *Anonymization* and *Turning off Data Collection*, remain underutilized and perceived as complex. We further show that organizational context is a key driver, with larger and regulated organizations exhibiting stronger adoption, whereas smaller ones face resource and expertise constraints. These findings highlight that effective privacy adoption depends on both developer capability and organizational support, motivating future work on longitudinal analyses and interventions to bridge this gap.

Acknowledgments. FUNCAP (BP6-00241-00276.01.00/25), PET-UFC, CNPq (404406/2023-8), CAPES (88881.879016/2023-01), and FAPESP (2023/00811-0).

References

Canedo, E. D., Bandeira, I. N., Calazans, A. T. S., Costa, P. H. T., Cançado, E. C. R., and Bonifácio, R. (2023). Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. *Requir. Eng.*, 28(2):177–194.

Corbin, J. and Strauss, A. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory. *Thousand Oaks*, 3:1–400.

Grissom, R. J. and Kim, J. J. (2005). *Effect sizes for research: A broad practical approach*. Lawrence Erlbaum Associates Publishers.

Iwaya, L. H., Babar, M. A., and Rashid, A. (2023). Privacy engineering in the wild: Understanding the practitioners' mindset, organizational aspects, and current practices. *IEEE Trans. Softw. Eng.*, 49(9):4324–4348.

Kempe, E. and Massey, A. (2021). Regulatory and security standard compliance throughout the software development lifecycle. In *54th HICSS*, pages 1–10. ScholarSpace.

Matos, A., Patrício, M., Nicolau, M. I., Canedo, E. D., Pereira, J. A., and Uchôa, A. (2025). Data privacy in software practice: Brazilian developers' perspectives. *J. Internet Serv. Appl.*, 16(1):299–319.

Schrader, P. G. and Lawless, K. A. (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. *Performance Improvement*, 43(9):8–15.

Tahaei, M., Frik, A., and Vaniea, K. (2021). Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proc. CHI Conf. Hum. Factors Comput. Syst.*, pages 693:1–693:15.

Whitley, E. and Ball, J. (2002). Statistics review 6: Nonparametric methods. *Critical care*, 6:1–5.