International Journal of Society Reviews (INJOSER) e-ISSN: 3030-802X
Vol. 2 No. 12, October 2025, pages: 2373~2380

FROM REGULATION TO LIABILITY: CHANGING DATA PRIVACY LANDSCAPE IN THE DIGITAL AGE

Rengga Yudha Santoso
Universitas PGRI Mpu Sindok
renggappkn@upms.ac.id

Yohana Rosita Dewi Mariyani
Universitas PGRI Mpu Sindok
yohanardm@upms.ac.id

Abstract

The rapid digital transformation has turned data privacy into a global strategic issue. Regulations such as the General Data Protection Regulation (GDPR) provide a comprehensive legal framework for the protection of personal data, but their effectiveness depends heavily on the ability of organizations to apply the principles of accountability and substantive responsibility. This research aims to analyze the paradigm shift from regulatory compliance (regulation-based) to organizational accountability (responsibility-based) in data privacy governance in the digital era. The approach used is qualitative with a systematic literature study method, reviewing Scopus-indexed scientific articles and the Web of Science published between 2015–2025, as well as policy reports from international institutions such as the OECD and EDPB. The analysis was carried out using thematic analysis techniques to identify the main patterns in the application of the principles of accountability, privacy by design, data protection impact assessment (DPIA), as well as social context and privacy ethics. The results show that the paradigm shift towards responsibility requires organizations not only to comply with formal regulations, but also to build an internal governance system that is able to proactively prove data protection. Mechanisms such as privacy by design and DPIA have proven effective in increasing transparency, risk mitigation, and public trust. In addition, the theory of Contextual Integrity and the Taxonomy of Privacy assert that privacy protection must consider social norms and ethical values, not just legal aspects. In the context of developing countries, including Indonesia, the implementation of privacy responsibilities still faces challenges such as limited institutional capacity, low digital literacy, and policy fragmentation. Therefore, it is necessary to strengthen independent supervisory institutions, increase public literacy, and integrate accountability principles in business strategies and technology design. This research confirms that the future of data protection lies in the balance between strong regulation and ethical responsibility of organizations. By internalizing the principles of accountability, organizations can build a transparent, ethical, and sustainable data ecosystem, while strengthening public trust in the digital age.

Keywords: *data privacy, accountability, responsibility, GDPR, data governance, privacy by design, DPIA, contextual integrity*

Introduction

The rapid development of digital technology has changed the way organizations collect, store, and process personal data. In the era of the digital economy, data has become a strategic asset that drives business innovation and analytics-driven decision-making. However, the massive use of data also poses a risk to the privacy rights of

individuals. According to Li et al. (2025), this shift drives the need for a protection framework that is not only based on legal regulations but also on the moral and ethical responsibilities of organizations in managing personal data. Thus, the data protection approach is no longer just reactive to the rule of law, but proactive in implementing accountability and privacy governance.

Initially, privacy protection focused on formal regulations such as the General Data Protection Regulation (GDPR) in the European Union which sets global standards for the control of personal data. However, research shows that legal compliance alone is often not enough to guarantee effective privacy protection (Ducato et al., 2020). Many organizations meet formal requirements without truly internalizing the values of accountability and transparency. Therefore, a new paradigm has emerged that emphasizes responsibility as part of corporate governance and business strategy.

The concept of responsibility in data privacy includes the principles of accountability, privacy by design, and data protection impact assessment (DPIA) which requires organizations to show concrete steps in protecting user rights (Iwaya et al., 2024). This approach requires evidence of implementation such as internal policies, audits, employee training, and secure technology systems. The OECD (2023) in its latest report also affirms that strengthening accountability through privacy management programs is an important element in a sustainable data protection ecosystem.

In addition, recent literature underscores the importance of understanding privacy as a contextual concept. Nissenbaum (2004) introduced the theory *of contextual integrity* which explains that privacy is not only about data ownership, but also the conformity of information flows with applicable social norms. When data is used outside of its social context, public trust in digital institutions and platforms can decrease significantly (Solove, 2006). Thus, organizational responsibility includes efforts to understand the social context and ethics of data use, not just compliance with legal texts.

In the context of globalization and cross-border digital transformation, privacy responsibilities are becoming increasingly complex. Kurtz and Wagner (2022) show that digital platform providers must integrate legal, technical, and social responsibilities in order to manage data across jurisdictions. This is a big challenge for organizations in developing countries, including Indonesia, which is implementing the Personal Data Protection Law (Law No. 27 of 2022). The implementation of responsibilities requires policy harmonization, digital literacy improvement, and technology adaptation in accordance with local values.

Thus, the shift from regulation to responsibility reflects the evolution of the data protection paradigm from normative compliance to substantive accountability. This approach places public trust at the core of sustainable data governance. This article will examine the dynamics of these changes by reviewing the current literature, analyzing best practices in various jurisdictions, and exploring their implications for developing countries such as Indonesia that are building the foundations of ethical and responsible data governance.

Literature Review

The Evolution of Data Privacy Regulation

Personal data protection is evolving from a *compliance-based legal system* to a more holistic, risk-based model. Regulations such as the General Data Protection Regulation (GDPR) are major milestones in asserting the rights of data subjects, establishing the obligations of data controllers, and introducing the principle of accountability (Li et al., 2025). GDPR changes the data protection paradigm from simply prohibiting breaches to risk management through prevention-oriented policy design. However, Ducato et al. (2020) highlight that the implementation of the GDPR still faces operational constraints, especially in terms of cross-jurisdictional compliance and varying interpretations.

In addition to GDPR, various countries have also adopted similar policies such as the California Consumer Privacy Act (CCPA) in the United States and the Personal Data Protection Act (PDPA) in Singapore. This policy affirms the importance of users' rights to access, rectification, and deletion of personal data. However, differences in legal context and institutional capacity in each country make the effectiveness of regulations highly dependent on the application of the principle of responsibility at the organizational level (OECD, 2023).

Principles of Organizational Accountability and Responsibility

Accountability is a key principle in modern privacy governance. Organizations are not only required to comply with regulations, but they must also be able to prove that they have taken adequate steps to protect personal data (Kurtz & Wagner, 2022). This approach is known as *demonstrable accountability*, which includes the implementation of internal policies, periodic audits, and training for employees. The OECD (2023) emphasizes that *privacy management programs* must include monitoring mechanisms, risk evaluation, and incident reporting to ensure ongoing protection. In the context of technology, organizational responsibility is also realized through the implementation of *privacy by design* and *privacy by default*, as described by Cavoukian (2011). This approach requires privacy protection to be part of the system design from the initial stage, not just an add-on after implementation. Thus, organizations are required to integrate privacy principles in product development processes, workflows, and business strategies.

Privacy Impact Assessment (PIA) dan Data Protection Impact Assessment (DPIA)

To strengthen organizational responsibility, GDPR introduces the *Data Protection Impact Assessment* (DPIA) mechanism as a risk evaluation tool before data processing is carried out. Iwaya et al. (2024) in their systematic review found that PIA/DPIA is effective in identifying potential violations and ensuring mitigation measures are implemented. However, its effectiveness is highly dependent on multidisciplinary engagement and an organizational culture that supports transparency. PIA/DPIA also helps demonstrate that organizations are not only compliant with the law, but also understand the social and ethical impacts of data processing activities.

Social and Ethical Context in Data Privacy

Nissenbaum (2004) introduced the theory of Contextual Integrity, which views privacy as the conformity of the flow of information to social norms and the context in which it is used. A breach occurs when information is used outside of applicable distribution norms. Meanwhile, Solove (2006) developed a privacy taxonomy that includes four main categories: collection, processing, dissemination, and intrusion. These two theories provide a conceptual basis for understanding why privacy responsibilities are not only legalistic, but also moral and social. By combining these theories, organizations can identify ethical risks that are not covered by formal regulations.

Challenges in Developing Countries

The implementation of privacy responsibility in developing countries faces structural challenges such as limited legal infrastructure, low digital literacy, and lack of oversight mechanisms (Kurtz & Wagner, 2022). In Indonesia, for example, even though Law No. 27 of 2022 on Personal Data Protection has been passed, challenges still arise in the technical and cultural implementation of the organization. Therefore, the integration of responsibilities into organizational governance is a strategic step to ensure substantive compliance and build public trust.

Synthesis Literature

From the literature review, it can be seen that the evolution of personal data protection demands synergy between regulation and responsibility. Regulation provides a legal framework, while responsibility ensures the implementation of privacy principles in real practice. The success of this model depends heavily on the application of accountability, impact assessment, and understanding of the social context. Thus, the focus of data protection shifts from formal compliance to substantive protection oriented towards trust and human values.

Research Methodology

This study uses a qualitative approach with a *systematic literature review design* to analyze the paradigm shift from regulation to responsibility in data privacy governance in the digital era. The qualitative approach was chosen because it is able to explore meanings, concepts, and patterns that emerge from various legal, social, and technological contexts (Creswell & Poth, 2018). This research does not focus on hypothesis testing, but on an in-depth understanding of the theoretical and implementive construction of the principle *of responsibility* in data protection policies.

Data Source

The data used in this study came from secondary literature in the form of Scopus and Web of Science indexed journal articles, academic books, and official reports from international institutions such as the OECD and the European Data Protection Board (EDPB). Articles are selected based on criteria: (a) published between 2015–2025, (b) address topics related to GDPR, accountability, privacy by design, data protection impact assessment, or contextual integrity, (c) are relevant to the theme of the transition from

regulation to responsibility in privacy governance. The search process was carried out using keywords such as: "GDPR accountability", "data protection governance", "privacy by design", "responsibility in data governance", and "contextual integrity".

Data Collection Techniques

Data collection was carried out through the following stages: Identification of the literature through the Scopus, ScienceDirect, and SpringerLink databases. Literature selection based on *inclusion criteria* and *exclusion criteria*. Data extraction to obtain key information related to the approaches, findings, and implications of each study. Thematic coding to group findings into key themes such as: regulation, responsibility, accountability, and the social context of privacy. This approach refers to the *systematic review* methodology developed by Tranfield, Denyer, & Smart (2003) to ensure traceability and transparency of the research process.

Data Analysis Techniques

Data analysis was carried out by *thematic analysis* to identify patterns and relationships between themes (Braun & Clarke, 2019). The analysis process includes six stages: (1) familiarization with the data, (2) initial coding, (3) theme identification, (4) theme review, (5) theme naming and definition, (6) compilation of the outcome narrative. Each of the main themes, such as "the role of GDPR in accountability", "challenges of implementing organisational responsibility", and "paradigm shift towards *privacy by design*", is analysed to find its conceptual meaning and practical implications.

Validity and Reliability

To ensure credibility and validity, this study uses source triangulation and trail audit techniques (Lincoln & Guba, 1985). Triangulation is done by comparing findings from various sources (academic articles, policy reports, and legal guidelines). In addition, the analysis process is systematically recorded so that it can be audited and replicated.

Research Limitations

This study has limitations in the availability of literature that explicitly discusses the transition from regulation to responsibility in the context of developing countries. Most studies still focus on the European context. However, these limitations provide opportunities for more empirical follow-up research with a case study approach in Indonesia post-implementation of PDP Law No. 27 of 2022.

Results and Discussion

Paradigm Shift: From Regulation to Responsibility

The results of the literature review show that personal data protection has undergone a significant transformation from a regulation-based paradigm to a responsibility-based paradigm. Regulations such as the General Data Protection Regulation (GDPR) position accountability as a key principle that requires organizations to not only comply with the rules, but also prove compliance through transparent internal mechanisms (Li et al., 2025). This principle shifts the approach from just formal compliance (*compliance-based*) to substantive *accountability*. Research by Ducato et al. (2020) shows

that the success of privacy protection now relies heavily on the ability of organizations to implement an integrated privacy management system, rather than just following a legal checklist.

Implementation of Accountability Principles in Organizational Practice

Literature findings reveal that the principle of accountability is realized through three main mechanisms: (1) Privacy by Design and by Default, (2) Data Protection Impact Assessment (DPIA), and (3) Privacy Management Program. According to Cavoukian (2011), *privacy by design demands* that privacy protection be an inherent part of system design and business processes from the early stages. Meanwhile, the study of Iwaya et al. (2024) shows that the implementation of DPIA is able to identify potential privacy risks early, increase risk awareness among stakeholders, and strengthen managerial accountability. The OECD (2023) also emphasizes the importance of periodic audits, employee training, and internal oversight as concrete evidence of organizational responsibility. However, the implementation of this principle is not always easy. Challenges arise from technological complexity, lack of expert human resources, and lack of alignment between cross-border regulations. Therefore, privacy responsibility requires a strategic commitment from top management, as well as the support of an organizational culture that supports data ethics.

The Social and Ethical Dimensions of Privacy Responsibilities

In addition to the legal aspect, responsibility in privacy also includes social and ethical dimensions. Nissenbaum (2004) through the theory of Contextual Integrity emphasizes that privacy violations often occur not because of violations of the law, but because of inconsistencies in the context of information distribution. For example, the use of health data for commercial purposes, even if legally permitted, can violate social norms and erode public trust. Solove (2006) added that privacy protection must take into account four main dimensions: collection, processing, dissemination, and intrusion. Thus, the organization's responsibilities go beyond legal obligations; It also includes moral sensitivity to societal expectations. Kurtz and Wagner (2022) emphasize that platform companies have a social responsibility to prevent misuse of data by third parties, through algorithmic audit mechanisms and ethical impact evaluations. This perspective transforms accountability into a multidimensional concept that encompasses law, technology, and morality.

Implementation Challenges and Gaps in Developing Countries

The results of the study show that in developing countries, including Indonesia, the implementation of privacy responsibilities still faces a number of obstacles. First, the institutional capacity of data supervision is still limited. Second, people's digital literacy is relatively low, causing difficulties in understanding personal data rights. Third, regulatory fragmentation and lack of inter-agency integration make the implementation of accountability principles less optimal. Although Law No. 27 of 2022 on Personal Data Protection has provided a legal framework, research shows that the success of such policies depends on the organization's commitment to implementing sustainable internal responsibilities. The OECD (2023) recommends that developing countries strengthen

privacy governance through: (a) strengthening independent supervisory bodies, (b) developing privacy management standards, and (c) cross-sectoral training. This is in line with the view of Li et al. (2025) that the sustainability of data governance cannot only rely on external regulations, but also the integration of responsibilities in business strategies.

Synthesis and Implications

Analysis of the literature findings shows that the shift from regulation to responsibility is not a replacement, but a reinforcement. Regulations provide a legal baseline, while the responsibility is to ensure their implementation ethically and sustainably. Successful organizations are those that are able to build a trust ecosystem, incorporating legal compliance, secure technology design, and transparency in communication with users. Implicitly, this study confirms that future privacy policies must integrate legal, technical, and social aspects and encourage *co-regulation* between governments, industry, and civil society.

Conclusion

This study concludes that the data privacy landscape in the digital age has undergone a significant transformation from a compliance-based regulatory paradigm to an accountability-based responsibility paradigm. Regulations such as GDPR have set global standards for the protection of personal data, but their effectiveness depends on the extent to which organizations are able to internalize accountability principles into internal governance (. A *responsibility-based approach* requires organizations to proactively demonstrate privacy protection through transparent policies, technologies, and practices. The concepts of privacy by design, privacy by default, and data protection impact assessment (DPIA) mechanisms play an important role in building a system that is secure and oriented towards individual rights. In addition, social approaches such as contextual integrity theory and privacy taxonomy broaden the understanding that privacy protection is not only legalistic, but also ethical and contextual. In the context of developing countries such as Indonesia, the existence of Law No. 27 of 2022 concerning Personal Data Protection is a step forward. However, its effectiveness still depends on institutional capabilities, people's digital literacy, and organizational commitment to implementing substantive responsibilities. This paradigm shift confirms that regulation is only the starting point; True success is determined by the extent to which the organization builds a culture of accountability and public trust.

References

Ducato, R., Forgó, N., & Others. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review, 36*(2), 105–118. https://doi.org/10.1016/j.clsr.2020.105392

Iwaya, L. H., Bernsmed, K., & Jaatun, M. G. (2024). Privacy impact assessments in the wild: A scoping review. *Journal of Responsible Technology, 18*, 100130. https://doi.org/10.1016/j.jrt.2024.100130

Kurtz, C., & Wagner, B. (2022). Accountability of platform providers for unlawful personal data processing. *Journal of Responsible Technology, 9*, 100020. https://doi.org/10.1016/j.jrt.2021.100020

Li, W., Cheng, L., & Li, Y. (2025). Mapping the empirical literature of the GDPR's (in-)effectiveness. *Computer Law & Security Review, 51*, 105996. https://doi.org/10.1016/j.clsr.2025.105996

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

OECD. (2023). *Report on the Implementation of the OECD Privacy Guidelines*. OECD Publishing.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.

Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information & Privacy Commissioner of Ontario.

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health, 11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE Publications.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Iwaya, L. H., Bernsmed, K., & Jaatun, M. G. (2024). Privacy impact assessments in the wild: A scoping review. *Journal of Responsible Technology, 18*, 100130. https://doi.org/10.1016/j.jrt.2024.100130