Journal of
Information System and Technology Auditing

Review Paper

Compliance Audit of Information Systems under General Data Protection Regulation (GDPR): Ensuring Compliance and Enhancing Personal Data Protection[1,2]

Bita Mashayekhi*[3] and Mahdi Safaei[4]

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 1, No. 1, Spring & Summer 2025
pp. 40-50

Received: 2025.02.16
Revised: 2025.08.07
Accepted: 2025.09.02

1. Introduction

The General Data Protection Regulation (GDPR) stands as one of the most significant regulatory measures in the realm of data protection, reflecting the growing recognition of personal data as a key resource in the modern digital economy. Implemented by the European Union in 2018, GDPR has brought about a transformative shift in organizational practices, compelling entities worldwide—regardless of geographic location—to reassess and restructure how they manage, store, and process personal data belonging to EU residents. Non-compliance exposes organizations to severe administrative fines (up to EUR 20 million or 4% of global turnover), reputational harm, and potential legal liabilities.

Despite existing research on GDPR and auditing, few studies have taken a truly holistic approach that merges legal, technical, and

[1] https://doi.org/10.22034/JISTA. 2025. 505314.1019
[2] Selected Paper of 2nd Congress of IT Audit and Digital Trust
[3] Prof, Department of Accounting, Faculty of Accounting and Financial Sciences, College of Management, University of Tehran, Tehran, Iran. (Corresponding Author) E-mail: mashaykhi@ut.ac.ir
[4] Ph.D. Student, Faculty of Accounting and Financial Sciences, College of Management, University of Tehran, Tehran, Iran. E-mail: safaei.mahdi@ut.ac.ir

organizational dimensions in a comparative framework. This extended abstract seeks to fill that gap by examining how GDPR requirements reshape information systems (IS) auditing and what novel strategies can be employed to navigate these complexities.

Objective and Scope

This research aims to provide a detailed examination of the compliance-based approach to GDPR within IS auditing, which differs from standard models by combining theoretical analysis and applied best practices. Specifically, we investigate how organizations align with GDPR mandates—ranging from data minimization and consent management to breach notification and privacy-by-design—while simultaneously addressing legal responsibilities, organizational governance, and technical safeguards. By exploring this intersection, we present a comparative view of practices and persistent challenges that offers a more integrated perspective than traditional studies focusing primarily on operational efficiency or baseline security controls.

Relevance to Information Systems Auditing

Traditional IS audits commonly focus on operational efficiency and baseline security controls. However, GDPR adds layers of complexity involving legal accountability, data subject rights, and the interplay of technology with evolving data ethics. Consequently, IS auditors must now incorporate privacy impact assessments, organizational governance checks, and vendor risk evaluations into their methodologies. This shift underscores the need for a robust auditing model that unifies technical safeguards—such as encryption, access controls, and intrusion detection systems (IDS)—with broader organizational strategies, including staff training, documented policies, and third-party oversight. In essence, while these technical measures are vital, they remain insufficient without a matching cultural and managerial framework, as further explored in subsequent sections.

2. MATERIALS AND METHODS

This study uses a comparative approach to examine the impact of GDPR on information systems auditing, as compliance with these regulations is a challenge not only at the EU level but also in many countries and international organizations. Comparative studies, which are widely observed in legal and regulatory research, allow for a more detailed analysis of regulatory gaps, implementation challenges, and successful strategies in the area of GDPR compliance.

In the present study, while analyzing the legal frameworks of GDPR, the impact of these regulations on information systems auditing practices and risk management strategies is examined. The structure of the article is set by focusing on the key principles of GDPR, the role of compliance auditing in ensuring data security, implementation challenges for organizations, and the future of auditing standards to provide a comprehensive picture of the relationship between GDPR and the audit profession.

In this regard, first, the legal foundations and principles of compliance auditing are examined. The implementation dimensions of monitoring and control at the levels of data governance, risk management, data subject rights, technical measures, and third-party oversight are analyzed. This structure is arranged in such a way that, while providing a comparative framework for examining the role of GDPR in compliance auditing, it also provides a comprehensive picture of the challenges, global standards, and future directions.

Compliance-Based Methodology

This research employs a qualitative review and compliance analysis methodology, integrating multiple sources to examine GDPR's impact on information systems auditing. The study relies on three primary sources: official regulatory texts and guidelines, peer-reviewed academic literature, and industry standards. Regulatory texts include GDPR itself, supplementary guidance issued by the European Data Protection Board (EDPB), and enforcement interpretations by data protection authorities (DPAs). Peer-reviewed studies provide insights into both theoretical and empirical dimensions of compliance auditing, offering critical perspectives on GDPR implementation challenges and solutions. Additionally, established industry frameworks such as ISO 27001

for information security management, COBIT for IT governance, and NIST cybersecurity guidelines serve as references to assess how organizations integrate GDPR requirements into standardized auditing practices.

Conceptual Framework

This study is structured around a four-layered conceptual framework that aligns GDPR compliance auditing with organizational governance, risk assessment, technical controls, and ongoing monitoring. The framework is designed to reflect the core structure of the paper and systematically evaluate how compliance audits address GDPR requirements.

First, the study examines the legal and governance framework, establishing the connection between GDPR mandates—such as data subject rights, accountability, and lawful processing requirements—and corporate data governance, audit policies, and IT control mechanisms. This section aligns with the discussion on data governance, compliance auditing, and regulatory enforcement, highlighting how organizational structures must integrate GDPR principles into their compliance strategies.

Second, it analyzes risk assessment and mitigation strategies, focusing on Data Protection Impact Assessments (DPIAs), risk categorization, and breach response mechanisms. This corresponds with sections covering risk management and compliance assessment, evaluating how audits identify vulnerabilities, enforce security measures, and reduce regulatory exposure.

Third, the study assesses technical and organizational controls, particularly the role of encryption, access control mechanisms, privacy-by-design principles, and compliance automation tools in strengthening GDPR compliance. This aligns with the discussion on technical safeguards, IT security auditing, and vendor risk management, demonstrating how audits verify the effectiveness of security protocols and privacy-enhancing technologies.

Finally, it explores continuous monitoring and compliance tracking, investigating how organizations implement real-time monitoring systems, audit trails, automated compliance reporting, and third-party oversight mechanisms to sustain long-term GDPR adherence. This aspect connects with sections on audit methodologies, governance models, and emerging trends in

compliance auditing, emphasizing the importance of proactive monitoring, AI-driven anomaly detection, and automated compliance verification.

By following this structured framework, the study provides a comprehensive, layered analysis of GDPR compliance auditing, ensuring that the interplay between legal mandates, risk assessments, security controls, and continuous oversight is systematically examined

3. RESULTS AND DISCUSSION

Governance and Data Management

The study finds that GDPR has fundamentally reshaped data governance models, mandating detailed record-keeping of data flows (RoPA), assigning Data Protection Officers (DPOs) in certain cases, and requiring strict retention policies. Audits thus transcend basic IT checks, incorporating governance criteria that cover managerial responsibilities and accountability. Organizations that excel in compliance often exhibit comprehensive policies clarifying data classification and retention periods, aligned with both operational needs and GDPR's storage limitation principle.

Risk Management and Breach Prevention

Risk assessment emerged as a core theme, with DPIAs taking center stage for high-risk data processing scenarios (e.g., large-scale profiling). Auditors play a pivotal role in validating if these DPIAs adequately measure potential damages, consider worst-case breach scenarios, and document mitigation steps. Despite widespread awareness, many SMEs struggle to operationalize risk management protocols, partly due to resource constraints and partly due to a lack of dedicated compliance expertise.

Privacy by Design and Default

Implementing privacy by design remains a notable challenge. While organizations acknowledge the necessity of embedding privacy controls (like anonymization, pseudonymization) into the earliest stages of system development, the review indicates that true end-to-end integration is uneven. Auditors frequently identify "bolt-on" privacy measures rather than privacy controls baked into development lifecycles. In industries dealing with large volumes of data, these gaps pose elevated compliance and ethical risks**.**

Third-Party Risk Assessment

The study repeatedly underscores how third-party vendors can create compliance blind spots if not properly audited. GDPR extends accountability to data processors, requiring revisiting contractual clauses, ensuring adequate security measures, and verifying sub-processors. A robust audit strategy checks for consistent vendor risk evaluations, regular compliance reporting, and immediate breach notification protocols. Failure in any of these areas can lead to material compliance violations.

Technical Measures: Encryption, Access Control, and Monitoring

The technical dimension of GDPR compliance frequently centers on encryption, least-privilege access control, and real-time monitoring. Organizations adopting ISO 27001 controls typically demonstrate stronger encryption key management and more systematic penetration testing. However, the review notes persistent issues with outdated cryptographic standards and insufficient multi-factor authentication (MFA), especially within legacy IT systems.

Organizational Measures: Training, Policies, and Culture

Effective GDPR compliance hinges on organizational culture. Regular training ensures employees understand fundamental GDPR principles like data minimization and breach reporting timelines. Audits highlight that even with robust technical safeguards, human error or lack of awareness can lead to non-compliance. Hence, staff education appears as a recurring recommendation in audit reports, emphasizing both legal obligations and best practices in data handling

4. CONCLUSION

Summary of Key Insights

This comparative study illustrates that aligning IS auditing with GDPR involves a holistic approach, integrating technical, legal, and organizational dimensions. Traditional audits, which primarily focused on IT controls, must now encompass deeper evaluations of data governance, privacy-by-design, and third-party risk management. Such a model allows organizations to not only comply with GDPR but also strengthen data protection, reduce operational risks, and enhance public trust.

Implications and Recommendations

The findings of this study suggest several strategic implications for organizations seeking to align their information systems auditing with GDPR compliance requirements. First, there is a need for integrated audit frameworks that align industry standards such as ISO 27001 and COBIT with GDPR's privacy and accountability principles. Organizations should refine their auditing methodologies to include privacy impact metrics, vendor oversight mechanisms, and rigorous incident response protocols. Second, the study highlights the importance of continuous monitoring in compliance enforcement. Integrating real-time compliance tracking, AI-driven anomaly detection, and automated breach notification systems can significantly enhance the effectiveness of GDPR audits by identifying irregularities in data processing before they escalate into regulatory violations.

Moreover, fostering a compliance-centric organizational culture is crucial in ensuring sustainable adherence to GDPR mandates. Beyond technical safeguards, organizations must prioritize staff training, clear governance structures, and well-documented policies to reinforce GDPR compliance at every operational level. Auditors must assess whether employees at all levels, from senior management to operational staff, fully understand and implement GDPR's core principles. Theoretically, these findings contribute to emerging research on privacy-by-design frameworks, while managerially, they offer CISOs and IT auditors practical pathways to embed GDPR metrics into governance, risk management, and compliance (GRC) systems.

Concluding Remarks

By systematically bridging the gap between regulatory prescriptions and practical auditing frameworks, organizations can develop comprehensive compliance strategies that anticipate both technological evolution and shifting legal landscapes. Ultimately, effective GDPR audits transcend box-checking exercises, shaping an environment where data protection is central to corporate governance and risk management. This approach not only fulfills legal mandates but fosters trust among consumers, regulators, and business partners—an invaluable asset in today's data-centric marketplace. In so doing, this extended abstract contributes a

structured, comparative lens on GDPR compliance, providing actionable pathways for auditors and organizations striving to meet stringent data protection requirements.

Keywords: Information Technology Audit (IT Audit), Compliance Audit, General Data Protection Regulation (GDPR)
JEL classification: *M42, M48, K20, L68*.

References

Alunge, R. (2021). Breach of security vs personal data breach: effect on EU data subject notification requirements. *International Data Privacy Law*, *11*(2), 163-181.

Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024). GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), 1338-1347.

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2023). A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, *4*(2), 100129.

Bertolaccini, L., Falcoz, P. E., Brunelli, A., Batirel, H., Furak, J., Passani, S., & Szanto, Z. (2023). The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database. *European Journal of Cardio-Thoracic Surgery*, *64*(3), ezad289.

Bowyer, A., Holt, J., Go Jefferies, J., Wilson, R., Kirk, D., & David Smeddinck, J. (2022, April). Human-GDPR interaction: practical experiences of accessing personal data. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-19).

Casutt, N., & Ebert, N. (2020, October). Data protection officers: Figureheads of privacy or merely decoration. In *Proc. 16th Eur. Conf. Manage., Leadership Governance* (p. 39).

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34*(2), 234-243.

Dashti, S., & Ranise, S. (2020). Tool-assisted risk analysis for data protection impact assessment. *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14*, 308-324.

Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk'in the General Data Protection Regulation. *Computer Law & Security Review*, *35*(6), 105342.

Dounis, N. P. (2017). GDPR Regulatory Compliance and the Role of Internal Audit: Theoretical and Practical Approach. *Int'l. In-House Counsel J.*, *11*, 1.

Duli, B. (2021). *Data transfers between the EU and US: the impact of schrems I and schrems II for cross-border data flows, privacy, and national security* (Doctoral dissertation).

Fahey, E., & Terpan, F. (2023). The future of the EU-US privacy shield. In *The Routledge Handbook of Transatlantic Relations* (pp. 221-236). Routledge.

Fakeyede, O. G., Okeleke, P. A., Hassan, A. O., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science*, *11*(11).

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process?. *Review of Accounting Studies*, *27*(3), 938-985.

Framework, B. E. (2015). The National Institute of Standards and Technology (NIST).

Geradin, D., Bania, K., & Karanikioti, T. (2022). The interplay between the Digital Markets Act and the General Data Protection Regulation. *Available at SSRN 4203907*.

Gilman, M. E. (2020). Five privacy principles (from the GDPR) the United States should adopt to advance economic justice. *Ariz. St. LJ*, *52*, 368.

Gobeo, A., Fowler, C., & Buchanan, W. J. (2022). *GDPR and Cyber Security for Business Information Systems*. River Publishers.

Goshadze, K. (2020). The Data Protection Officer (DPO)-Ensuring Greater Data Protection Compliance. *Law & World*, *14*, 41.

Hijmans, H., & Raab, C. D. (2018). Ethical Dimensions of the GDPR. *Commentary on the General Data Protection Regulation, Cheltenham: Edward Elgar (2018, Forthcoming)*.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

I. G. P. Team (2025). EU general data protection regulation (GDPR): an implementation and compliance guide. Packt Publishing Ltd.

Kasirzadeh, A., & Clifford, D. (2021, July). Fairness and data protection impact assessments. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 146-153).

King, D. (2019). Data classification: A means to an end. *Journal of Data Protection & Privacy*, *2*(4), 324-330.

Knoke, F., & Nwankwo, I. (2022). Managing Data Protection Compliance through Maturity Models: A Primer. *Eur. Data Prot. L. Rev.*, *8*, 536.

La Torre, M., Botes, V. L., Dumay, J., & Odendaal, E. (2021). Protecting a new Achilles heel: the role of auditors within the practice of data protection. *Managerial Auditing Journal*, *36*(2), 218-239.

Lachaud, E. (2020). ISO/IEC 27701 standard: Threats and opportunities for GDPR certification. *Eur. Data Prot. L. Rev.*, *6*, 194.

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices. *Administrative Sciences*, *14*(10), 238.

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2022). Towards privacy compliance: A design science study in a small organization. *Information and Software Technology*, *146*, 106868.

Mahmodi Parchini, M. , Riazi, L. and Pour Ebrahimi, A. (2025). Comparison of Personal Data Protection Laws: Unique General Regulations under the European Union's General Data Protection Regulation (GDPR) and United States Laws. *News Science Quarterly (NS)*, *13*(4), 204-224. (In Persian)

Nannini, L., Bonel, E., Bassi, D., & Maggini, M. J. (2024). Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act. *AI and Ethics*, 1-29.

Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. In *The ethics of information technologies* (pp. 141-178). Routledge.

Pandit, H. J. (2023). Making sense of Solid for data governance and GDPR. *Information*, *14*(2), 114.

Regulation, G. D. P. (2019). *GDPR. 2019*.

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: a global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences*, *6*(1), 73-88.

Rhahla, M., Allegue, S., & Abdellatif, T. (2021). Guidelines for GDPR compliance in Big Data systems. *Journal of Information Security and Applications*, *61*, 102896.

Rosenberger, A., Shvartzshnaider, Y., & Sanfilippo, M. (2021). Digital Contact Tracing in the EU: Data Subject Rights and Conflicting Privacy Governance. *Proceedings of the Association for Information Science and Technology*, *58*(1), 819-821.

Saltarella, M., Desolda, G., & Lanzilotti, R. (2021, July). Privacy design strategies and the GDPR: A systematic literature review. In *International Conference on Human-Computer Interaction* (pp. 241-257). Cham: Springer International Publishing.

Sargiotis, D. (2024). Data Governance Frameworks: Models and Best Practices. In *Data Governance: A Guide* (pp. 165-195). Cham: Springer Nature Switzerland.

Sayankar, V. N. (2013). A Review on Information Systems Audit. *Research Journal of Engineering and Technology*, *4*(3), 103-106.

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An analysis of economic impact on IoT industry under GDPR. *Mobile Information Systems*, *2018*(1), 6792028.

Sharifi Kia, M. A. and Shabani Jahromi, F. (2022). The Condition of Considering the Data Personal in Cyberspace Comparative Review of European General Data Protection Regulation and Iranian law. *Private Law*, *19*(1), 221-245. (In Persian)

Sim, J., Kim, B., Jeon, K., Joo, M., Lim, J., Lee, J., & Choo, K. K. R. (2023). Technical requirements and approaches in personal data control. ACM Computing Surveys, 55(9), 1-30.

Sovrano, F., Sapienza, S., Palmirani, M., & Vitali, F. (2022). Metrics, explainability and the European AI act proposal. *J*, *5*(1), 126-138.

Tamburri, D. A. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, *91*, 101469.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5-8.

Trakman, L., Walters, R., & Zeller, B. (2020). Digital consent and data protection law–Europe and Asia-Pacific experience. *Information & Communications Technology Law*, *29*(2), 218-249.

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, *15*(1), 83-106.

Zakerhosseini, S. (2020). Review the performance of the audit process based on auditors' knowledge of information technology. *Journal of Accounting and Management Vision*, *3*(33), 73-98. (In Persian)

Zhou, L., Wub, Y., Wang, H., Yao, Y., Wangd, Y., & Jiao, Z. (2024, October). Information Protection Impact Assessment in China. In Proceedings of the 4th International Conference on Management Science and Software Engineering (ICMSSE 2024) (Vol. 244, p. 88). Springer Nature.

Zichichi, M., Ferretti, S., D'Angelo, G., & Rodríguez-Doncel, V. (2022). Data governance through a multi-DLT architecture in view of the GDPR. Cluster Computing, 25(6), 4515-4542.