Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

RESEARCH ARTICLE

Research Article

PERSONAL DATA PROTECTION IN VIETNAM'S PUBLIC ADMINISTRATION: A COMPARATIVE ANALYSIS WITH THE EU GENERAL DATA PROTECTION REGULATION

Nguyen Thi Thuy, Tran Kim Lieu* and Vu Van Tuan

DOI:
https://doi.org/10.33327/AJEE-18-9.4-a0002011

Date of submission: 18 Jun 2026
Date of acceptance: 03 Aug 2026
Online First Publication: 26 Sep 2026

Disclaimer:
The authors declare that the opinion and views expressed in this manuscript are free of any impact of any organizations.

ABSTRACT

Background: *The expansion of data-driven governance has intensified personal data protection within public administration. Although contemporary data protection regimes share common principles, their operation in the public sector remains uneven. This study examines how the General Data Protection Regulation (GDPR) and Vietnam's Law No. 91/2025/QH15 regulate personal-data processing by public authorities and what their differences imply for institutional accountability and individual rights.*

Method: *The study assesses normative architecture, institutional responsibilities, and compliance frameworks in the two legal systems. It combines systematic comparative legal analysis of primary legal instruments with thematic analysis of secondary sources, allowing for both structural comparison and contextual interpretation across jurisdictions. The doctrinal analysis identifies formal legal*

requirements, while observations concerning implementation are derived from secondary literature and are not presented as original empirical findings.

Results and Conclusions: *The findings demonstrate that robust legal frameworks do not ensure effective protection. The two systems show partial convergence in general data-protection principles but significant differences in public-sector processing, impact assessment, internal compliance functions, supervisory independence, and enforcement. Differences in administrative capacity, organizational culture, oversight arrangements, and digital governance strategies identified in the secondary literature may influence compliance. Accordingly, formal convergence should not be interpreted as institutional or functional equivalence. The research concludes that meaningful personal data protection in public administration depends on the alignment of law, institutions, and governance practices. Context-sensitive harmonization, supported by effective oversight and administrative capacity, is essential to safeguarding individual rights and enhancing trust in data-driven public governance.*

1 INTRODUCTION

The swift digitization in the field of public administration has transformed the way governments obtain, process, store, and disseminate personal information. Data collection has become the centrepiece of public service delivery and regulatory enforcement as governments implement e-governance systems, interoperable databases, digital identification technologies, and algorithmic tools. The promise of digital administration includes options for the government to operate more efficiently and in ways that provide better service to the public. However, the potential for unlawful data collection and retention, function creep, and unlawful surveillance becomes much more pronounced. As such, data collection and surveillance have become the centrepiece of public administration and regulatory compliance, and the same can be said for the significant impact this has on the private sector and the non-consensual collection and processing of personal data and the use of data in vertical administration. Data-driven technologies and automated decision-making have transformed the public sector and are reshaping administrative actions.[1] As personal data protection becomes more prioritized, emerging regulations have framed the protection of personal data as a fundamental, or quasi-fundamental, right.

1 Zaheer Allam and Zaynah A Dhunny, 'On Big Data, Artificial Intelligence and Smart Cities' (2019) 89 Cities 80 <https://doi.org/10.1016/j.cities.2019.01.032> accessed 20 April 2026; Irina Pencheva, Marc Esteve and Slava Jankin Mikhaylov, 'Big Data and AI – A Transformational Shift for Government: So, What Next for Research?' (2020) 35(1) Public Policy and Administration 24 <https://doi.org/10.1177/0952076718780537> accessed 20 April 2026.

The EU's General Data Protection Regulation (GDPR)[2] is a milestone in the development of a comprehensive pan-European framework for balancing the protection of rights, with accountability obligations imposed on data controllers.[3] Furthermore, the GDPR has had significant extraterritorial influence and has served as a benchmark for new data protection regimes globally.[4] The spread of GDPR-inspired data protection laws has revealed friction. Although laws can appear to be converging, divergent conditions of administrative ability, legal culture, and design of institutions often render protective frameworks largely ineffective. Such friction often shows itself more on the surface of data protection law that intersects with public administration and the protection of the public interest and the administrative efficiency of the governance system.[5]

This study is theoretically positioned within comparative public law and the rights-based theory of data protection. It draws from the work of the contextual and functional approach to comparative law as expounded by Samuel.[6] This approach posits that legal provisions should be understood in relation to the issues they seek to solve and the specific context (here, *institutional*) within which they operate. Consequently, the study examines legal provisions related to the protection of personal data as legal instruments that are situated within the context of public administration. Additionally, the study views the protection of personal data through the prism of human dignity, the right to self-determination, and democracy. Despite the expansion of literature on data protection and digital governance, there are a number of notable gaps. The literature seems to be concerned with the regulation

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 <http://data.europa.eu/eli/reg/2016/679/oj> accessed 20 April 2026.

3 Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28(1) Information & Communications Technology Law 65 <https://doi.org/10.1080/13600834.2019.1573501> accessed 20 April 2026; M Laxmi Jagannadh and S Sumitra, 'Comparative Analysis of Data Protection and Privacy Laws' (2025) 23(s6) Lex Localis – Journal of Local Self-Government 8565 <https://doi.org/10.52152/51h4tr43> accessed 20 April 2026.

4 Suk Kyoung Kim, Min Jae Park and Jae Jeung Rho, 'Does Public Service Delivery Through New Channels Promote Citizen Trust in Government? The Case of Smart Devices' (2019) 25(3) Information Technology for Development 604 <https://doi.org/10.1080/02681102.2017.1412291> accessed 20 April 2026; Cedric Ryngaert and Mistale Taylor, 'The GDPR as Global Data Protection Regulation?' (2020) 114 American Journal of International Law 5 <https://doi.org/10.1017/aju.2019.80> accessed 20 April 2026.

5 Kornraphop Kawintiranon and Yaguang Liu, 'Towards Automatic Comparison of Data Privacy Documents: A Preliminary Experiment on GDPR-Like Laws' (*arXiv*, 1 May 2021) arXiv:2105.10117 [cs.CL] <https://doi.org/10.48550/arXiv.2105.10117> accessed 20 April 2026; Christopher Kuner, 'Protecting EU Data Outside EU Borders under the GDPR' (2023) 60(1) Common Market Law Review 77, <https://doi.org/10.54648/cola2023004> accessed 20 April 2026.

6 Geoffrey Samuel, *An Introduction to Comparative Law Theory and Method* (Bloomsbury Publishing 2014).

of the private sector, while the position of public authorities is undertheorized.[7] In comparative research, there is a tendency to focus on regulatory convergence and the GDPR, while other highly relevant factors, including compliance, administrative rationale, institutional capacity, and the regulation of biopolitics, remain overlooked. Moreover, research on emerging and transitional legal systems is often too descriptive, documenting legal reforms while lacking a robust analysis of the underlying institutional framework and the potential practical ramifications of such reforms.[8] Accordingly, this study asks: How do the GDPR and Vietnam's Law No. 91/2025/QH15[9] regulate personal-data processing by public authorities, and what do their differences imply for institutional accountability and individual rights?

Addressing these gaps, this study contributes to the literature in three ways. First, it reconceptualizes the problem of personal data protection as a problem of administrative law and public governance, rather than as a descriptive problem of legal compliance. It shifts the focus to public administration and reveals the ways in which data protection obligations interact with administrative frameworks, professional cultures, and routines of decision making. Second, it merges systematic comparative legal scholarship with qualitative thematic analysis in line with the methodological guidance provided by Braun and Clarke.[10] Such a blend of approaches allows for the recognition of patterns, tensions, and normative propositions in a legal system, and analytical transparency and rigor. Third, its original contribution is a focused examination of Vietnamese public-sector processing, particularly the relationship between formal legal convergence and differences in institutional accountability, oversight, and implementation. The study concludes that personal data protection in public administration requires both the adoption of more sophisticated legal frameworks and the embedding of these frameworks within administrative practice. By

7 Sean Sirur, Jason RC Nurse and Helena Webb, 'Are We There Yet? Understanding the Challenges Faced in COmplying with the General Data Protection Regulation (GDPR)' (*arXiv*, 22 August 2018) arXiv:1808.07338 [cs.CY] <https://doi.org/10.48550/arXiv.1808.07338> accessed 20 April 2026; Ewa Wanda Ziemba, 'The Contribution of ICT Adoption to the Sustainable Information Society' (2019) 59(2) Journal of Computer Information Systems 116 <https://doi.org/10.1080/08874417.2017.1312635> accessed 20 April 2026.

8 Bach Thi Nha Nam and Nguyen Ngoc Phuong Hong, 'Addressing the Challenges of Data Privacy Protection Law in Vietnam' (2023) 39(1) VNU Journal of Science: Legal Studies 30 <https://doi.org/10.25073/2588-1167/vnuls.4413> accessed 20 April 2026; Nguyen Ho Bich Hang, 'Addressing Fragmentation in Vietnam's Data Protection Laws: Recommendations for a Unified Legal Framework' (2024) 11(2) Vietnamese Journal of Legal Sciences 14 <https://doi.org/10.2478/vjls-2024-0008> accessed 20 April 2026; Tố Trang Lâm, 'Some Legal Aspects of Personal Data Protection in the World: Experience for Vietnam' (2024) 10(1) Cogent Social Sciences 2414872 <https://doi.org/10.1080/23311886.2024.2414872> accessed 20 April 2026.

9 Law of the Socialist Republic of Vietnam no 91/2025/QH15 'On Personal Data Protection' (adopted 26 June 2025) <https://english.luatvietnam.vn/dan-su/law-on-personal-data-protection-law-no-91-2025-qh15-405135-d1.html> accessed 20 April 2026.

10 Virginia Braun and Victoria Clarke, *Thematic Analysis: A Practical Guide* (SAGE 2021).

making a systematic comparison of how the GDPR and Vietnam's legal framework regulate and enforce data protection in the public sector, the study seeks to explore the strengths and weaknesses of data protection reforms in a contemporary data state.

2 METHODS

This research employs a systematic comparative legal research design, informed by the conceptual approach developed by Samuel.[11] Comparative analysis is used to examine how the European Union and Vietnam regulate personal data protection in public administration when confronted with similar governance challenges. Rather than relying on a purely textual comparison of legal provisions, the study adopts a functional and contextual perspective. This allows the analysis to account for institutional settings, administrative structures, and regulatory objectives that shape the operation of data protection norms within each legal framework.[12] The comparison is organized around the following analytical dimensions relevant to public-sector data processing: legal bases and public-sector exceptions, data-subject rights, the distribution of controller and processor responsibilities, impact assessment, internal compliance functions, oversight, breach notification, cross-border transfers, sanctions, and AI-related processing.[13] Primary legal instruments were examined doctrinally and compared under each dimension. The analysis draws on secondary sources, including scholarly publications, policy documents, and authoritative reports. Sources were included where they directly addressed public-sector data protection, institutional accountability, or implementation in the EU or Vietnam.

In addition, the study applies thematic analysis to secondary materials, following the methodological guidance provided by Braun and Clarke.[14] This method is used to identify recurring themes and interpretive patterns related to administrative capacity, rights protection, and regulatory effectiveness. Coding is conducted iteratively through initial coding, comparison of recurring patterns, and review and definition of the principal themes. Legal propositions derived from primary instruments are treated as doctrinal findings. Statements concerning administrative practice or regulatory effectiveness are derived from secondary sources and are not presented as original empirical findings; no interviews, surveys, or observational data were collected.[15] By integrating thematic analysis with comparative legal reasoning, the research moves beyond descriptive comparison and

11 Samuel (n 6).

12 ibid

13 Regulation (EU) 2016/679 (n 2); Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152/1 <http://data.europa.eu/eli/reg/2022/868/oj> accessed 20 April 2026; Law of the Socialist Republic of Vietnam no 91/2025/QH15 (n 9).

14 Braun and Clarke (n 10).

15 ibid

offers interpretive insight into the underlying assumptions and tensions within data protection governance. Together, the methods distinguish formal legal requirements from literature-based observations about their implementation.

3 RESULTS AND DISCUSSION

3.1. Normative Architecture for the Protection of Personal Data in the Public Sector

The normative legal structure for the protection of personal data in the public sector administration reflects the underlying constitutional, administrative, and regulatory traditions that govern the exercise of public power in a given jurisdiction. This architecture determines the normative status of data protection, the obligations imposed on public authorities and the enforceable rights available to individuals.[16] For the purposes of this study, the comparison is specifically between the GDPR framework applicable to public authorities in the European Union and Vietnam's Law on Personal Data Protection, Law No. 91/2025/QH15, together with its implementing Decree No. 356/2025/ND-CP.[17] Both Vietnamese instruments took effect on 1 January 2026. Constitutional protection may take the form of an autonomous data-protection right or broader guarantees concerning privacy and confidentiality. In the legal framework of the EU, the protection of personal data is recognized as an autonomous fundamental right under Article 8 of the Charter of Fundamental Rights[18] and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU)[19], separate from, but closely associated with the right to respect for private and family life under Article 7 of the Charter. By contrast, Article 21 of Vietnam's Constitution[20] protects private life, personal and family secrets, and the confidentiality of communications but does not expressly formulate an autonomous right to personal-data protection. Such constitutional recognition influences the interpretation of the GDPR,

16 Cong Tran Quoc Le, Viet Dung Tran and Dao Phuong Thuy Nguyen, 'Global Norms and Regional Innovation: GDPR, Evolution of Data Protection in ASEAN and the Legal Trajectory of AI in Vietnam' (2025) 15(3) TalTech Journal of European Studies 250 <https://doi.org/10.2478/bjes-2025-0039> accessed 20 April 2026.

17 Decree of the Socialist Republic of Vietnam no 356/2025/ND-CP 'Detailing Certain Provisions and Measures for Implementing the Law on Personal Data Protection' (adopted 31 December 2025) <https://vanban.chinhphu.vn/?pageid=27160&docid=216387> accessed 20 April 2026.

18 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2012_326_R_0391_01> accessed 20 April 2026.

19 Treaty on the Functioning of the European Union (consolidated version) [2012] OJ C 326/47 <http://data.europa.eu/eli/treaty/tfeu_2012/oj> accessed 20 April 2026.

20 Constitution of the Socialist Republic of Vietnam (adopted 28 November 2013) <https://www.constituteproject.org/constitution/Socialist_Republic_of_Vietnam_2013> accessed 20 April 2026.

limits the exercise of public power and enables individuals to seek administrative and judicial protection.[21] Public authorities are, therefore, not merely subject to general privacy expectations; they exercise legally bounded powers when collecting, using, sharing, and retaining personal data.

The absence of an autonomous constitutional data-protection right does not, by itself, determine whether a legal framework is coherent or effective. The legal protection of data is often scattered among a variety of sector-specific laws, administrative rules, and guidelines that are internal to certain public authorities. Even if such legal frameworks include a certain data-protection principle, their effectiveness depends on statutory hierarchy, institutional design, administrative discretion, and available remedies. The scattering of data protection norms may create a lack of clarity about the legal grounds for processing data, the breadth of administrative discretion, and the lack of action on the part of the administration to protect the rights of individuals.[22] Within this context, fragmentation may reduce legal clarity and enforceability; however, its effects must be assessed within the particular legal system. Vietnam previously relied on a more fragmented combination of sector-specific legislation and Decree No. 13/2023/ND-CP.[23] That decree represented an important initial consolidation of personal-data rules, but it operated at the level of delegated legislation rather than a dedicated statute. The enactment of Law No. 91/2025/QH15 and Decree No. 356/2025/ND-CP has since established a more unified statutory framework. Decree No. 356/2025/ND-CP replaced Decree No. 13/2023/ND-CP from 1 January 2026, although the former decree remains historically relevant to understanding Vietnam's regulatory development.

A key element of the normative structure pertains to the articulation, as well as the legal standing, of fundamental principles of data protection. The principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability have gained acceptance across most contemporary data protection frameworks. However, the differences in their expression and legal effect are significant. Under Article 5 GDPR, these principles are expressly codified as binding processing requirements. They apply to both public and private data controllers, subject to context-specific provisions, restrictions, and exceptions. This consistency fosters legal certainty and settles the compliance obligations of public authorities in the processing of

21 Hoofnagle, van der Sloot and Borgesius (n 3); Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca (eds), *The Evolution of EU Law* (3rd edn, OUP 2021) 902, <https://doi.org/10.1093/oso/9780192846556.003.0029> accessed 20 April 2026.

22 Nguyen (n 8); Tong Thi Phuong Thao, 'Laws on Personal Data Protection in Vietnam Today' (2025) 14(1) International Journal of Engineering Inventions 47 <https://www.ijeijournal.com/v14-i1.html> accessed 20 April 2026.

23 Decree of the Socialist Republic of Vietnam no 13/2023/ND-CP 'Protection of Personal Data' (adopted 17 April 2023) <https://vanban.chinhphu.vn/?pageid=27160&docid=207759> accessed 20 April 2026.

personal data, irrespective of the sectorial context.[24] In addition, the principles are more than interpretive aids; they are prescriptive, and, thus, sufficiently_solid to sustain administrative and judicial oversight. Vietnam establishes its own principles under Article 3 of Law No. 91/2025/QH15, but their wording and structure are not identical to Article 5 GDPR. Vietnam's 2025 Law similarly establishes enforceable rights and obligations, including rights to information, consent or refusal, withdrawal of consent, access, rectification, deletion, restriction, objection, complaint, litigation, and compensation under Article 4. It imposes statutory responsibilities on controllers and processors under Article 37. The two frameworks converge in recognizing legally enforceable protection, but differ in how particular obligations and public-sector exceptions are structured.

The principle of legality plays an essential role within the regulatory structure of the protection of personal data in the public administration sector. Under Articles 5(1)(a) and 6(1) GDPR, every controller, whether public or private, must identify a lawful basis for each processing operation.[25] The public-sector distinction is not that only public authorities require a legal basis. Rather, public authorities commonly rely on processing that is necessary to comply with a legal obligation under Article 6(1)(c), or to perform a task carried out in the public interest or in the exercise of official authority under Article 6(1)(e). Article 6(3) further requires the basis for such processing to be established in Union or Member State law. In addition, public authorities may not rely on the legitimate-interests ground in Article 6(1)(f) when processing data in the performance of their public tasks.[26] Consent is not legally excluded from public-sector processing, but it will frequently be inappropriate where a significant imbalance of power means that the individual cannot freely refuse without adverse consequences. EU public authorities should rely on consent only where the conditions of freely given, specific, informed and unambiguous agreement can genuinely be satisfied. In most mandatory administrative relationships, Articles 6(1)(c) and 6(1)(e) provide more appropriate legal bases.

24 Reece Iriye, 'The European Union General Data Protection Regulation' (*Stimson Center*, 24 September 2024) <https://www.stimson.org/2024/the-european-union-general-data-protection-regulation/> accessed 20 April 2026; Christina Tikkinen-Piri, Anna Rohunen and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2017) 34(1) Computer Law & Security Review 134 <https://doi.org/10.1016/j.clsr.2017.05.015> accessed 20 April 2026.

25 Frederik J Zuiderveen Borgesius and Wilfred Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust' (*arXiv*, 9 October 2025) arXiv:2510.08247 [cs.CY] <https://doi.org/10.48550/arXiv.2510.08247> accessed 20 April 2026; Hoofnagle, van der Sloot and Borgesius (n 3).

26 Bach and Nguyen (n 8); Dao Kim Anh, Pham Xuan Phong and Phan Duong Quang, 'Enhancing the Responsibilities of Data Controllers in Vietnam: Insights from the European General Data Protection Regulation' (2024) 40(1) VNU Journal of Science: Legal Studies 90 <https://doi.org/10.25073/2588-1167/vnuls.4610> accessed 20 April 2026; Tu Thien Huynh, 'Everyone is Safe Now: Constructing the Meaning of Data Privacy Regulation in Vietnam' (2024) 11(4) Asian Journal of Law and Society 530 <https://doi.org/10.1017/als.2024.36> accessed 20 April 2026.

Acknowledging this asymmetry, many data-protection frameworks limit the use of consent in administrative situations and instead focus on a legal basis of statutory power, public interest, or legal obligation. Nonetheless, not all legal systems provide this clarity. In some places, it is still possible to use consent to describe a situation that is, in fact, not voluntary, which is contrary to the intention of data protection law.[27] The normative architecture includes structures related to the distribution of responsibilities within public administration. Modern data-protection regimes increasingly require public authorities to document processing, assess risks, implement technical and organizational safeguards and establish internal compliance arrangements. Under the GDPR, accountability requires controllers not only to comply with the principles in Article 5(1), but also to demonstrate compliance under Article 5(2). Public authorities must ordinarily designate a data protection officer under Article 37(1)(a). High-risk processing may require a data protection impact assessment under Article 35. These provisions are particularly relevant to automated decision-making, systematic monitoring, large-scale databases and the processing of sensitive information.[28] Vietnam's framework similarly requires agencies and organizations to designate a qualified personal-data-protection unit or responsible personnel under Article 33(2), while Article 21 provides for personal-data-processing impact-assessment dossiers. Conversely, Vietnamese internal personnel or units should not be presented as functionally equivalent to GDPR DPOs: Articles 38 and 39 GDPR expressly regulate the DPO's organizational position, resources, absence of instructions, protection from dismissal and advisory and monitoring functions, whereas Article 33 of the Vietnamese Law does not reproduce all of those guarantees. Yet, Article 21(6) exempts competent state agencies from the statutory impact-assessment requirement. This is an important point of divergence from the GDPR and should not be obscured by a general statement that the two systems impose equivalent accountability duties. The Vietnamese exemption may reduce administrative burdens for state bodies, but it possibly raises questions about how risks arising from large-scale governmental processing are assessed and documented through alternative mechanisms.

27 Pusp Raj Joshi and Shareeful Islam, 'E-Government Maturity Model for Sustainable E-Government Services from the Perspective of Developing Countries' (2018) 10(6) Sustainability 1882 <https://doi.org/10.3390/su10061882> accessed 20 April 2026; Magdalena Jurczuk and Maria Suprunowicz, 'Consent in Data Privacy: A General Comparison of GDPR and HIPAA' (2024) 16 Przegląd Prawniczy Uniwersytetu Im Adama Mickiewicza 173 <https://doi.org/10.14746/ppuam.2024.16.07> accessed 20 April 2026.

28 Malang BS Bojang, 'Challenges and Successes of E-Government Development in Developing Countries: A Theoretical Review of the Literature' (2019) 3(4) International Journal of Research and Innovation in Social Science 410 <https://rsisinternational.org/virtual-library/papers/challenges-and-successes-of-e-government-development-in-developing-countries-a-theoretical-review-of-the-literature/> accessed 20 April 2026; Paul Voigt and Axel von Dem Bussche, 'Practical Implementation of the Requirements under the GDPR' in Paul Voigt and Axel von Dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 245 <https://doi.org/10.1007/978-3-319-57959-7_10> accessed 20 April 2026.

As reported in the secondary literature, the integration of accountability requirements and obligations within administrative law is patchy. In legal systems that have a well-established culture of managerial discretion or hierarchical command, the protection of rights through procedures is viewed as a burden. This can turn compliance systems into a box-ticking exercise that is overly focused on documentation, as opposed to the identification and mitigation of risks. These are literature-based observations about implementation rather than doctrinal findings derived from the legal instruments. This institutional problem may arise under either framework and should be distinguished from differences in the legal texts themselves. Enforcement and remedies comprise yet another important element of the normative framework.[29] The effectiveness of data-protection rights depends on accessible complaint procedures, meaningful corrective powers and judicial remedies. Under Articles 51 and 52 GDPR, Member States must establish supervisory authorities that act with complete independence. Article 58 grants those authorities investigative and corrective powers, while Articles 77–79 provide rights to lodge complaints and seek effective judicial remedies. Vietnam adopts a structurally different oversight model. Article 33 identifies the specialized personal-data-protection authority within the Ministry of Public Security as part of the personal-data-protection force, and Article 36 designates the Ministry of Public Security as the principal body responsible to the Government for state management of personal-data protection. This model does not reproduce the GDPR requirement of a structurally independent supervisory authority. Nevertheless, Article 4 of the Vietnamese Law expressly grants data subjects rights to complain, report violations, initiate legal proceedings and claim compensation in accordance with applicable law.[30] The relevant comparative issue is not the complete absence of oversight or remedies, but the difference between independent regulatory supervision in the EU and executive state-management supervision in Vietnam.

Data-protection law must operate together with administrative-law safeguards. Requirements concerning transparency, reasoned decision-making, access to information, complaint procedures and judicial review convert abstract rights into practical protection. When a public authority informs an individual why and under what legal authority data are processed, the individual is better able to assess the legality of that processing and challenge it where necessary. Otherwise, where procedures are inaccessible or exceptions are drafted too broadly, statutory data-protection rights may remain difficult to exercise. A comparative perspective further underscores the impact of

29 Bojang (n 28); Guangwei Hu and others, 'The Influence of Public Engaging Intention on Value Co-Creation of E-Government Services' (2019) 7 IEEE Access 111145 <https://doi.org/10.1109/ACCESS.2019.2934138> accessed 20 April 2026.

30 Kuner (n 5); Sirur, Nurse and Webb (n 7).

digital governance on normative formation.[31] The reliance of the public sector on automated, data-driven, and interoperable database decision-making systems poses a challenge to normative traditions. The GDPR addresses some of these risks through the principles of necessity, proportionality, data protection by design, impact assessment, and restrictions on solely automated decisions. Article 23 permits legislative restrictions on certain rights only when the restriction respects the essence of fundamental rights and is necessary and proportionate to a recognized public objective.

Secondary literature identifies continuing challenges concerning algorithmic transparency, collective data, and systemic risks. While some jurisdictions have optimized their systems to address these challenges, others remain reliant on administrative systems designed for their analogue predecessors.[32] This gap raises concerns about the sustained effectiveness of outdated administrative systems. These implementation-related observations should be supported by the relevant secondary sources and should not be presented as conclusions derived solely from the statutory comparison. The normative structure on the protection of personal data in public administration is intricate and composed of various elements. This structure consists of the elements of the constitution, the design of the statute, the mechanisms of enforcement, and the traditions of administration. Although paradigm shifts around the core principles of data protection have occurred, widespread variations continue in terms of legal consistency, institutional coherence, and the synergy of practical enforcement. These variations have important consequences on how individual rights are recognized and the legitimacy of data-driven public administration. Hence, the need to comprehend the structure is critical for evaluating both the robust and frail facets of the contemporary data protection mechanisms in the administrative state.

3.2. The Architecture of Institutional Accountability and the Oversight Frameworks for the Governance of Data Protection in the Public Sector

The effectiveness of data protection in the public sector depends partly on how legal and institutional frameworks allocate responsibilities among public authorities, internal compliance personnel, and external oversight bodies. These frameworks determine the accountability of public administrators, how responsibilities are to be operationalized, and the capacity of oversight and accountability bodies to monitor, investigate, and

31 Maribel González Pascual, 'Public Administrations and Data Protection' in Karl-Peter Sommermann, Adam Krzywoń and Cristina Fraenkel-Haeberle (eds), *The Civil Service in Europe: A Research Companion* (Routledge 2025) 649 <http://dx.doi.org/10.4324/9781003458333-40> accessed 20 April 2026; Dennis Rosenberg, 'Use of E-Government Services in a Deeply Divided Society: A Test and an Extension of the Social Inequality Hypotheses' (2019) 21(2) New Media & Society 464 <https://doi.org/10.1177/1461444818799632> accessed 20 April 2026.

32 Luca Nannini and others, 'Beyond Phase-In: Assessing Impacts on Disinformation of the EU Digital Services Act' (2024) 5(2) AI and Ethics 1241 <https://doi.org/10.1007/s43681-024-00467-w> accessed 20 April 2026; Pencheva, Esteve and Mikhaylov (n 1).

respond to unlawful activities associated with data processing. Secondary literature reviewed in this study suggests that variations in institutional design often account for the disparate outcomes that can be observed in different jurisdictions despite the imposition of the same legal rules. A public authority acts as a controller where it determines, alone or jointly, the purposes and means of processing; depending on the arrangement, it may instead act as a processor or joint controller. This role comes with legal obligations, including the protection of data, the implementation of administrative safeguards, and cooperation with the competent data-protection authority. Under the GDPR, these obligations apply to both public and private controllers, while certain institutional duties apply specifically to public authorities. In Vietnam, the corresponding responsibilities are principally governed by Law No. 91/2025/QH15 and its implementing Decree No. 356/2025/ND-CP.[33] Public authorities are expected to include data protection as part of their usual administrative duties and not as an external obligation. The distribution of duties in public administration is diverse. In some cases, responsibility for data protection is spread out, with individual public authorities retaining responsibility for their own processing activities. This model promotes data-protection compliance, but it can lead to uneven practices across administrative bodies. Conversely, some jurisdictions have adopted centralized models, leading to greater consistency across public authorities and a more coherent implementation of the administrative framework. Although centralization may improve compliance in some areas, it may be less responsive to the operational needs of particular administrative sectors.[34]

One of the most striking aspects of recent developments in data protection is the emergence of internal compliance functions in public authorities. The assignment of specific personnel or units within public administrations to deal with data protection issues is symptomatic of a shift towards more preventive and organizationally accountable forms of data protection. The idea is to internalize data protection-related expertise to help public authorities comply with the law. Under Article 37(1)(a) GDPR, a data protection officer must generally be designated where processing is carried out by a public authority or body, except for courts acting in their judicial capacity. Article 33 of Vietnam's Law similarly requires agencies and organizations to designate qualified personal-data-protection personnel or units, or to engage a qualified service provider. Nonetheless, these Vietnamese personnel or units should not be presented as functionally equivalent to GDPR DPOs. Articles 38 and 39 GDPR expressly protect the DPO's organizational position, resources, freedom from instructions and monitoring, and advisory functions, whereas Article 33 of the Vietnamese Law does not reproduce all of those guarantees. Secondary literature indicates that internal

33 Hoa Thanh Ha and Tuan Van Vu, 'Potential Conflicts in Personal Data Protection under Current Legislation in Vietnam Compared with European General Data Protection Regulation' (2024) 7(3) Access to Justice in Eastern Europe 505 <https://doi.org/10.33327/ajee-18-7.3-a000304> accessed 20 April 2026; Hoofnagle, van der Sloot and Borgesius (n 3).

34 González Pascual (n 31).

compliance functions are likely to be more effective when they are structurally supported by organizations or public authorities and are provided with the necessary resources and an organizational culture that enables them to influence compliance practices. Compliance personnel may have limited capacity to identify or act on unlawful processing where they lack sufficient resources, access to decision-making, or organizational independence.[35] The role of external oversight is as important as internal compliance functions. Independent authorities are crucial for effective oversight and the protection of the rights and freedoms of data subjects. Their responsibilities include supervising compliance, processing of complaints, conducting inquiries, and adopting enforcement measures. Under Articles 51 and 52 GDPR, Member States must establish supervisory authorities that act with complete independence, while Article 58 grants them investigative and corrective powers.[36] This is especially necessary in the public domain where the imbalance of power between citizens and the public authority is more pronounced.

Vietnam adopts a different institutional model. Article 33 of Law No. 91/2025/QH15 places the specialized personal-data-protection authority within the Ministry of Public Security, while Article 36 identifies the Ministry of Public Security as the principal body responsible to the Government for state management of personal-data protection, subject to the respective responsibilities of the Ministry of National Defense, other ministries, and provincial People's Committees. Unlike the GDPR, the Vietnamese Law does not expressly establish a supervisory authority with complete institutional independence from the executive.[37] This difference should not be understood as the presence of oversight in the EU and its absence in Vietnam. Rather, it reflects a distinction between the GDPR's independent supervisory-authority model and Vietnam's executive state-management model. Judicial control is equally important in data protection governance systems. Courts offer an indispensable venue for the interpretation of data protection standards, the resolution of conflicts and the clarification of the boundaries of administrative discretion. In situations where judicial oversight is possible and efficient, it reinforces accountability by allowing individuals whose personal data were unlawfully processed to challenge the system and obtain compensation. The existence of formal rights and accountability mechanisms is insufficient if judicial protection is not easily available due to procedural obstacles, the high cost of litigation, or rules of standing that limit access. The relationship between courts and supervisory bodies may determine whether formal accountability mechanisms provide effective protection in practice.[38]

In addition to formal oversight organizations, mechanisms of political and administrative accountability deserve attention. Data protection governance through oversight of administrative activities and responses to persistent problems can be influenced by

35 Voigt and von Dem Bussche (n 28).
36 Kuner (n 5).
37 Sirur, Nurse and Webb (n 7).
38 Streinz (n 21).

parliamentary committees, audit institutions, and offices of the ombudsman. Although these bodies may not possess specialized data-protection expertise, their involvement is particularly important where public-sector processing is connected with policy implementation, public expenditure, and the exercise of statutory powers.[39] The following observations concerning technological coordination, outsourcing, and institutional culture are derived from secondary literature rather than primary legal instruments. Oversight responsibilities and institutional accountability have been made more complex by new digital technologies and the sharing of data across sectors. Responsibility for compliance and accountability has been diffused by the use of interoperable systems and databases across multiple administrative systems. In such a situation, overlapping responsibilities and ill-defined accountability may create governance gaps. Some jurisdictions have created enhanced coordination mechanisms across supervisors and specific accountability in the instances of collective data processing. In contrast, others have stuck to compartmentalized institutional frameworks that have become ineffective in dealing with current data governance issues.[40] The interface between the public and private sectors presents institutional challenges. Public authorities have a growing dependence on private providers for the supply of digital infrastructure, data analytics, and service provision. Although contractual frameworks may allocate responsibilities between public supervisors and private contractors, effective oversight still requires public authorities to possess the legal and technical capacity to audit contractors, obtain relevant information, and enforce contractual obligations. Outsourcing does not remove the public authority's accountability for personal-data processing.[41] Furthermore, institutional culture is a crucial factor in shaping the oversight of institutional mechanisms. Where legal frameworks exist, if supervisory bodies adopt a collaborative or deferential stance towards public administration, enforcement may be slow and selective.

A culture that prioritizes oversight may increase compliance, even in the absence of wide-ranging enforcement. These factors may not be adequately captured by a purely doctrinal approach, but they are vital in explaining the mechanisms in place to ensure compliance with data protection.[42] Ultimately, the impact of institutional responsibilities and oversight mechanisms hinges on the transparency of the processes and the involvement of the public. Trust and legitimacy are fostered through access to information, reporting

39 Marijn Janssen and others, 'Trustworthiness of Digital Government Services: Deriving a Comprehensive Theory Through Interpretive Structural Modelling' (2018) 20(5) Public Management Review 647, <https://doi.org/10.1080/14719037.2017.1305689> accessed 20 April 2026.

40 Pencheva, Esteve and Mikhaylov (n 1).

41 Danny S Guamán and others, 'Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications' (2023) 130 Computers & Security 103262 <https://doi.org/10.1016/j.cose.2023.103262> accessed 20 April 2026.

42 Nam Giang Do and Khoi Trong Dao, 'More than Just Privacy: Latent Policies for the Codification of Vietnamese Personal Data Protection Law' (2025) 15(3) International Data Privacy Law 268 <https://doi.org/10.1093/idpl/ipaf013> accessed 20 April 2026; Huynh (n 26).

mechanisms of the supervisory bodies, and active engagement of the public in the complaint mechanisms. When oversight mechanisms are unclear and difficult to navigate, people are less likely to assert their rights. The secondary literature reviewed in this study suggests that oversight mechanisms focusing on transparency are more likely to increase compliance and strengthen the protective side of the data protection law in the public administration.[43] Accordingly, although the GDPR and Vietnamese law both establish internal compliance and external oversight arrangements, they differ principally in the institutional independence and location of the supervisory function. These differences are directly relevant to the balance between administrative efficiency, accountability, and the protection of individual rights.

3.3. Administrative Implementation and Compliance in Public-Sector Data Protection Frameworks

Administrative implementation concerns the process through which legal data-protection norms are translated into the everyday practices of public authorities. Unless expressly attributed to a primary legal instrument, the implementation-related observations in this section are derived from secondary literature and are not presented as original empirical findings. This process is neither immediate nor uniform. It is dependent on organizational capacity, professional culture, techno-legal infrastructure, and tensions between legal requirements and operational demands. This is why public authorities can operate under similar normative frameworks but still achieve compliance differently. These differences demonstrate that the implementation of data-protection rules is as important as their formal legislative design. A characteristic trait of administrative implementation is the formulation of internal frameworks that put into practice the principles of data protection. Increasingly, public authorities turn to internal policies, handbooks, ethical guidelines, and standard operating procedures that direct staff on how to lawfully handle personal data. They act as vital links between the statutes and routine administrative choices. They are particularly important in data-heavy sectors, such as taxation, social security, and population databases. Frontline staff routinely deal with large amounts of personal data, often under time and performance pressures.

Comparative studies, however, show that internal rules vary in legal and operational quality because of uneven institutional awareness, legal knowledge, and management commitment.[44] Policies that merely restate legal provisions without explaining how they apply to administrative tasks have limited practical value. Training and capacity building

43 Liang Ma and Yueping Zheng, 'National E-Government Performance and Citizen Satisfaction: A Multilevel Analysis Across European Countries' (2019) 85(3) International Review of Administrative Sciences 506 <https://doi.org/10.1177/0020852317703691> accessed 20 April 2026.

44 Andreea Buruiana, 'Personal Data Protection in the Digitalization Process of the Public Administration' (2024) 11(2) European Journal of Law and Public Administration 15 <https://doi.org/10.18662/eljpa/11.2/227> accessed 20 April 2026; Tong (n 22).

are another important aspect of administrative compliance. Legal requirements are of little value if public employees do not have a practical working understanding of the principles of data protection for everyday tasks. In environments with systematic and ongoing data protection training, data protection is likely to be viewed as part of a professional ethos, and not a burden from an external regulatory body. Such training combines examples from specific sectors, thus empowering employees to identify data protection issues associated with everyday administrative tasks. By contrast, environments with training that is infrequent, limited to upper management, or excessively theoretical typically have compliance that is reactive and shallow. This is evident in data-heavy environments, such as healthcare, social services, and digital identity, where operational imperatives often take precedence over data-subject rights.[45]

Compliance outcomes can be shaped by documentation and records-management practices. Current frameworks require public authorities to record data processing, legal grounds, their protections, and the sharing of data. These obligations are intended to improve transparency, support internal and external oversight, and enable supervisory authorities to evaluate compliance. Under Articles 5(2) and 30 GDPR, public authorities must be able to demonstrate compliance and, subject to limited exceptions, maintain records of processing activities. Vietnam's Law No. 91/2025/QH15 likewise imposes compliance responsibilities on controllers and processors and requires personal-data-processing impact-assessment documentation under Articles 21 and 37. The two frameworks recognize documentation as an accountability mechanism, although their specific requirements and public-sector exceptions differ. Operational compliance in Vietnam includes cross-border-transfer requirements under Article 20, breach notification under Article 23, and sanctions under Article 8. These provisions operate alongside the Data Law, Decree No. 165/2025/ND-CP, the Law on Electronic Transactions, and the Law on Artificial Intelligence. Compliance-focused documentation can promote learning and the management of institutional risks.[46] For this reason, the practice typically leads to a growing perception of documentation activities as burdensome. This perception is more frequent in publicly funded bodies constrained in their resources. Where documentation requirements focus solely on producing evidence of formal compliance, there is a risk that records will become disconnected from substantive administrative decision-making. The secondary literature reviewed indicates that, in many cases, 'paper compliance' does very little to reduce risks to individual rights.[47]

45 Sohail Raza Chohan and Guangwei Hu, 'Strengthening Digital Inclusion Through E-Government: Cohesive ICT Training Programs to Intensify Digital Competency' (2022) 28(1) Information Technology for Development 16, <https://doi.org/10.1080/02681102.2020.1841713> accessed 20 April 2026; Janssen and others (n 39).

46 Le Vinh Chau, Nguyen Xuan Quang and Ngo Khanh Tung, 'Processing of Children's Personal Data: A Comparative Study of the EU Legal Framework and Vietnamese Law' (2025) 15(2) TalTech Journal of European Studies 56 <https://doi.org/10.2478/bjes-2025-0020> accessed 20 April 2026.

47 Sirur, Nurse and Webb (n 7).

Impact assessments demonstrate both promise and pitfalls. Impact assessments are meant to encourage public bodies to understand and mitigate risks to specific rights before they start processing or using new technologies. Impact assessments could reinforce system design, proportionality and accountability, if done properly. A significant legal difference arises between the two frameworks. Article 35 GDPR requires a data protection impact assessment where processing is likely to result in a high risk to individual rights and freedoms, including when processing is undertaken by a public authority. Article 21 of Vietnam's Law requires a personal-data-processing impact-assessment dossier but exempts competent state agencies from this requirement under Article 21(6). This exemption is particularly relevant to evaluating risk management in Vietnamese public administration and should be distinguished from the GDPR approach.[48] Another aspect of administrative implementation is transparency and communication with data subjects. Public authorities have an obligation to inform the public in a clear, timely, and accessible manner regarding data processing, individual rights, and their questions and concerns. However, the obligation to be transparent is in conflict with communication processes that tend to be bureaucratic and prioritize legal concerns, protections to the organization, and technical completeness over communication. Hence, Article 12 GDPR expressly requires information to be provided in a concise, transparent, intelligible, and easily accessible form. Article 4 of Vietnam's Law recognizes the rights to information, access, rectification, deletion, restriction, objection, complaint, litigation, and compensation. The practical comparison concerns not simply whether rights are formally recognized, but whether public authorities establish accessible procedures through which rights can be exercised.[49]

When data subjects exercise their rights, they reveal the operational limitations of public administration. Rights such as access, rectification, erasure, and objection require public authorities to develop internal processes to respond in accordance with the applicable legal procedures and time limits. In public administrations marked by decentralized data systems, legacy databases, and divided organizational units, finding and amending personal data is often complex and resource-consuming. Delays, incomplete replies, and inconsistent responses are frequent. These problems are particularly pronounced where multiple organizations are involved in joint processing or where information is retained in outdated or incompatible systems. These challenges highlight the need for organizational structures, information systems, and legal requirements to be aligned.[50] The growing dependence of public authorities on external service providers impacts compliance practices. The outsourcing of digital infrastructure, cloud services, and data analytics adds new layers of legal and operational complexity.

48 Voigt and von Dem Bussche (n 28); Pencheva, Esteve and Mikhaylov (n 1).

49 Huynh (n 26); Thi Tuyet Dung Thai, Van-Duong Nguyen and Van-Lam Nguyen, 'A Comparative Study of Cross-Border Data Transfer Regulations in Vietnam and Singapore Ensuring the Protection of Privacy' (2025) 26(2) Asia-Pacific Journal on Human Rights and the Law 81 <https://doi.org/10.1163/15718158-26020001> accessed 20 April 2026.

50 Bach and Nguyen (n 8); Nguyen (n 8).

Where public authorities act as controllers and private providers act as processors, contracts or other binding legal instruments allocate their respective responsibilities, and effective oversight requires public authorities to possess the legal and technical skills necessary to monitor and enforce contractual obligations. In many administrations, these skills are lacking. Consequently, public authorities may have bound themselves contractually to processors and relied on vendor certifications, without having substantive control of processing activities. Such dependence raises questions regarding accountability and the erosion of public control over sensitive data.[51] Under Article 28 GDPR, controllers may use only processors that provide sufficient guarantees and must regulate processing through a binding contract or other legal act. Article 37 of Vietnam's Law similarly allocates responsibilities between controllers and processors. In both systems, outsourcing does not eliminate the public authority's responsibility to supervise processing carried out on its behalf. The significance of organizational culture is often underappreciated, but it is critical to compliance outcomes. When data protection is seen as a barrier to efficiency and innovation, compliance is viewed as a defensive and minimalist practice. Rather than focusing on protecting individual rights, officials seek to avoid penalties. In contrast, when data protection is seen as a component of governance values, such as accountability, service, and trust, officials are more likely to comply. Differences in organizational culture may help explain why similar regulatory obligations produce different outcomes across public administrations.[52]

The digital age adds complexity to administrative compliance. Automated decision making, interoperability of databases, and large-scale sharing of data complicate compliance models that rely on well-defined process steps and control points. Responsibility may be within the operational, technical, and contractual layers of an organization. Under the GDPR, Articles 22, 25, and 35 address aspects of automated decision-making, data protection by design, and high-risk processing. Article 30 of Vietnam's Law specifically regulates personal data processed through big data systems, artificial intelligence, blockchain, virtual environments, and cloud computing. It requires purpose limitation, necessity, appropriate safeguards, and risk classification for artificial intelligence systems. Nevertheless, Article 30 is a personal-data-protection provision rather than a comprehensive AI regulatory framework and should be read together with the Law on Artificial Intelligence. The existence of statutory requirements does not establish their effectiveness in practice; implementation depends on technical capacity, internal review, and effective supervision.[53]

The enforcement ecosystem plays a vital role in administrative compliance. Secondary literature reports positive compliance developments in regulatory environments where enforcement agencies interact with public administrations through guidance, audits, dialogue, and enforcement actions. Such interactions enable public administrations to

51 Guamán and others (n 41).
52 Ma and Zheng (n 43).
53 Nannini and others (n 32).

navigate regulatory ambiguity and institutionalize compliance. Weak, inconsistent, or politically limited enforcement tends to reinforce the notion that compliance with data protection regulations is merely a formality. Under Articles 57 and 58 GDPR, supervisory authorities combine advisory, investigative, and corrective functions. In Vietnam, supervision and state-management responsibilities are principally exercised through the Ministry of Public Security under Articles 33 and 36 of Law No. 91/2025/QH15. As discussed in Section 3.2, this institutional distinction may affect how compliance by public authorities is guided, investigated, and enforced.[54] Administrative implementation demonstrates the limitations of relying exclusively on formal legal rules. Under both the GDPR and Vietnamese law, effective public-sector compliance depends on organizational capacity, professional culture, appropriate technology, meaningful documentation, risk assessment, and sustained oversight. The principal differences concern state-agency impact assessments and the institutional structure through which public-sector compliance is supervised and enforced.

3.4. Analytical Framework for Legal Integration and Advancing Public Data Governance Systems

The analysis of public administration's legal perspectives on data protection reveals new avenues and challenges for integrating contemporary governance systems. Both the GDPR and Vietnam's Law No. 91/2025/QH15, together with Decree No. 356/2025/ND-CP, recognize core data-protection principles and impose obligations on public-sector processing. Nonetheless, the way in which these frameworks structure, interpret, and enforce those obligations differs significantly. Therefore, legal integration requires more than the formal alignment of legal texts; it requires attention to institutional design, administrative capacity, and enforcement structures. At the level of principles, comparative analysis shows partial convergence on the core elements of data protection, such as lawfulness, proportionality, purpose limitation, accountability, and transparency. These elements have become a part of the shared regulatory lexicon, and increasingly influence legislative reforms outside of their initial jurisdictions. The regulatory framework established by the European Union has been particularly influential and serves as both a point of reference and a source of inspiration for policymakers aiming to update their data protection legislation.[55] Furthermore, principle-based convergence does not imply that governance outcomes may converge. Legal homogeneity often obscures variation in the implementation of norms.

A purely formal approach to harmonization has significant structural limitations. Although legislative alignment may improve legal certainty and facilitate cross-jurisdictional cooperation, it does not by itself address differences in administrative

54 Kuner (n 5); Hoofnagle, van der Sloot and Borgesius (n 3).

55 Hoofnagle, van der Sloot and Borgesius (n 3); Ryngaer and Taylor (n 4).

systems and institutional arrangements. Disparities in the resources, technology, professional capacity, and organizational structures of public administration can result in the same legal duty being applicable and enforceable in one context while remaining ineffective or merely symbolic in another. Substantive differences in implementation may persist despite formal legal convergence. The comparison developed in Sections 3.1–3.3 illustrates this distinction. The GDPR requires independent supervisory authorities and ordinarily requires public authorities to appoint data protection officers, whereas Vietnam places specialized oversight principally within the executive state-management structure led by the Ministry of Public Security. Vietnam's framework exempts competent state agencies from the personal-data-processing impact-assessment requirement, unlike the GDPR's risk-based approach to high-risk public-sector processing. The secondary literature reviewed suggests that, in the absence of a corresponding degree of investment in administrative systems, harmonization is likely to increase the governance gap.[56] Additionally, there is tension between administrative autonomy at the national level and regulatory consistency at the international level, and this is particularly concerning for the harmonization of data protection. In some areas, externally imposed data protection standards seem to infringe on policy making and administrative processes. This is particularly true for issues of public sensitivity, such as the protection of the state, the management of migration, and the administration of social welfare, where policymakers need to exercise discretion and make decisions quickly. In such matters, the legislation may be implemented selectively or only at a formal level. Conversely, where harmonization standards are perceived to be for the betterment of governance, the protection of rights, and the enhancement of public confidence, authorities are more likely to adopt them as legitimate governance standards.[57]

The comparative approach focuses on the interplay between the harmonization of data protection and administrative reform priorities on a broader scale. A considerable number of public administrations pursue digital transformation strategies aimed at improving efficiency, system interoperability, and evidence-based policymaking. Although such goals may seem to be aligned with the principles of innovation and effectiveness, in the absence of adequate data protection, they may create conflicts. Legal harmonization is not sufficient to resolve such conflicts. Governance frameworks must deal with the protection of personal data in advance and in an integrated way with digital strategies, procurement frameworks, and organizational structures.[58] Another area where comparative variances have pronounced governance implications is oversight and coordination mechanisms. As processing public sector data becomes more inter-organizational and cross-sectoral, oversight fragmentation becomes more problematic. Some jurisdictions have sought to

56 Sirur, Nurse and Webb (n 7).

57 Huynh (n 26); Janssen and others (n 39).

58 Mark Esposito, Yusaf Akbar and Francis Xavier Campbell, *Digitalization in Emerging Economies* (CUP 2025); Pencheva, Esteve and Mikhaylov (n 1).

address this by enhancing coordination among oversight bodies, clarifying roles in multi-party data processing, and establishing frameworks for collaborative regulation. Other jurisdictions continue to operate under oversight arrangements that are, by design, administratively siloed. These patterns suggest that achieving effective harmonization is more complex than simple uniformity; it requires governance arrangements that integrate both stasis and adaptive oversight to mirror evolving administrative arrangements.[59]

From a comparative perspective, the challenges posed by legal translation in the governance of data protection are more pronounced. While the adoption of legal ideas, institutional frameworks, or enforcement models from other jurisdictions can facilitate the development of a regulatory framework and demonstrate a commitment to aligning with international standards, it can result in regulatory misalignment if the transplant is not crafted with sufficient contextual awareness.[60] Accountability frameworks designed for sophisticated, resource-rich environments may operate poorly in fragmented or resource-constrained settings. Formal compliance cannot compensate for the absence of effective governance structures and may create the appearance of harmonization without equivalent protection in practice.[61] Ideally, if harmonized rules are properly reflected in administrative practices, they would support participatory governance and trust in public authorities. Weak and inconsistent practices, however, may increase administrative opacity and arbitrariness. The comparison indicates that governance outcomes depend less on the formal incorporation of shared principles than on the extent to which those principles are integrated into administrative culture and decision-making processes.[62]

Democratic accountability has emerged as a key concern in harmonized data protection governance. As regulatory frameworks become more complex and technically sophisticated, there is a risk that governance shifts away from political and public scrutiny towards expert-driven regulation. While expertise is indispensable in managing complex data processing systems, excessive technocratization may reduce transparency and weaken democratic oversight. The secondary literature reviewed suggests that governance arrangements combining independent supervision with parliamentary scrutiny and judicial review are more resilient and enjoy greater public legitimacy over time.[63] Technological change further complicates harmonization dynamics. Automated decision-making, artificial intelligence, and large-scale data analytics challenge legal concepts developed for earlier administrative models. The GDPR addresses these developments through instruments including data protection by design, impact assessment, and restrictions on

59 Kuner (n 5).

60 Do Hong Quyen and Bui Ngoc Linh, 'Discussing Personal Data Protection During Arbitration Proceedings and Lessons for Vietnam' (2024) 9(6) European Journal of Social Sciences Studies 75 <http://dx.doi.org/10.46827/ejsss.v9i6.1691> accessed 20 April 2026.

61 Bach and Nguyen (n 8); Nguyen (n 8).

62 Ma and Zheng (n 43).

63 González Pascual (n 31); Streinz (n 21).

certain automated decisions. Vietnam's Article 30 specifically addresses personal data processed through big data systems, artificial intelligence, blockchain, virtual environments, and cloud computing. However, Article 30 is a personal-data-protection provision rather than a comprehensive AI regulatory framework. It should be read together with the Law on Artificial Intelligence and, where applicable, the Data Law, Decree No. 165/2025/ND-CP, and the Law on Electronic Transactions. Nevertheless, the existence of technologically responsive provisions does not ensure equivalent implementation, particularly where institutional capacity and independent supervision differ.

Comparative analysis suggests that harmonization efforts must remain flexible if they are to remain relevant in rapidly evolving digital environments.[64] Accordingly, harmonization should pursue convergence in substantive protection without requiring identical institutional arrangements in every jurisdiction. Sufficient flexibility is necessary to accommodate administrative traditions, institutional capacity, and continuing technological development. In the comparison between the GDPR and Vietnam's current framework, meaningful integration depends on whether shared legal principles are supported by effective internal compliance, credible oversight, accessible remedies, and sustained administrative reform.

4 CONCLUSION

This study has undertaken the analysis of personal data protection in public administration through a comparative, governance-based approach. The study illustrates that, within public sector administration, data protection cannot be achieved solely through the design of legislation, but through the legal, institutional, and practical interplay of the day-to-day operation of public administrators. Therefore, protecting personal data in the context of governance should be regarded as an essential feature of contemporary administrative law and the exercise of public authority. While there seems to be partial convergence on the fundamental principles of data protection across jurisdictions, this analysis shows that there remains significant divergence on the structures and processes that integrate these principles into public administration. In particular, the GDPR and Vietnam's framework differ in public-sector processing, impact-assessment requirements, internal compliance functions, supervisory independence, and enforcement. Institutional responsibilities and oversight mechanisms are crucial in closing the gap between law and practice. In the public sector, oversight, internal compliance mechanisms, and judicial remedies are important elements of data-protection governance, although their institutional form differs between the two systems. However, these mechanisms are most effective where there is institutional autonomy, sufficient resources, and unambiguous mandates.

64 Nannini and others (n 32).

The analysis of the administrative implementation shows the limitations of strictly legalistic or enforcement-centered approaches. As these implementation findings are derived from secondary literature rather than original empirical research, they should be interpreted as contextual observations. The integration of data protection into everyday administrative practices relies on compliance activities such as training, documentation, risk assessment, and transparency. Yet, these activities are influenced by competing demands, such as efficiency, the delivery of a particular policy, or political responsiveness. With the growing adoption of digital technologies in public administration, traditional compliance approaches based on separate processing and linear decision-making are under increasing pressure. Such a shift demands new governance strategies that weave data protection considerations into digital strategy, procurement, organizational design, and systems design from the outset, rather than as after-the-fact considerations. While principles may be common, administrative capability and institutional culture may differ, and rigid harmonization may disregard these differences. By contrast, regulatory harmonization, which permits contextual differences and allows for adaptive learning may support substantive rather than merely formal protection. The protection of personal data is transforming the public authorities' understanding of legitimacy, transparency, and the interface of governance with the citizen. The integration of data protection norms into the administration of processes can strengthen governance, fairness, and trust in public administration. On the contrary, poor implementation may contribute to administrative opacity and arbitrariness, especially in areas of governance where there is heavy reliance on data.

This study urges a rethinking of data protection as a fundamental element of democratic governance. The unanswered questions posed by automated decision-making, artificial intelligence, and massive data analytic processing remain only partly addressed by existing legal frameworks. Comparative insights may help identify alternative governance models, highlight relevant and adaptable features of models, and position such models within the limits of the contexts. The comparative and contextual approach can assist researchers and policymakers in navigating the challenges of balancing the protection of privacy and the administrative innovation for the digital age. This approach is critical to data protection as a means of upholding individual rights and enabling honest governance.

REFERENCES

1. Allam Z and Dhunny ZA, 'On Big Data, Artificial Intelligence and Smart Cities' (2019) 89 Cities 80 <https://doi.org/10.1016/j.cities.2019.01.032> accessed 20 April 2026
2. Anh DK, Phong PX and Quang PD, 'Enhancing the Responsibilities of Data Controllers in Vietnam: Insights from the European General Data Protection Regulation' (2024) 40(1) VNU Journal of Science: Legal Studies 90 <https://doi.org/10.25073/2588-1167/vnuls.4610> accessed 20 April 2026

3. Bach TNN and Nguyen NPH, 'Addressing the Challenges of Data Privacy Protection Law in Vietnam' (2023) 39(1) VNU Journal of Science: Legal Studies 30 <https://doi.org/10.25073/2588-1167/vnuls.4413> accessed 20 April 2026
4. Bojang MBS, 'Challenges and Successes of E-Government Development in Developing Countries: A Theoretical Review of the Literature' (2019) 3(4) International Journal of Research and Innovation in Social Science 410 <https://rsisinternational.org/virtual-library/papers/challenges-and-successes-of-e-government-development-in-developing-countries-a-theoretical-review-of-the-literature/> accessed 20 April 2026
5. Borgesius FJZ and Steenbruggen W, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust' (*arXiv*, 9 October 2025) arXiv:2510.08247 [cs.CY] <https://doi.org/10.48550/arXiv.2510.08247> accessed 20 April 2026
6. Braun V and Clarke V, *Thematic Analysis: A Practical Guide* (SAGE 2021)
7. Buruiana A, 'Personal Data Protection in the Digitalization Process of the Public Administration' (2024) 11(2) European Journal of Law and Public Administration 15 <https://doi.org/10.18662/eljpa/11.2/227> accessed 20 April 2026
8. Chohan SR and Hu G, 'Strengthening Digital Inclusion Through E-Government: Cohesive ICT Training Programs to Intensify Digital Competency' (2022) 28(1) Information Technology for Development 16 <https://doi.org/10.1080/02681102.2020.1841713> accessed 20 April 2026
9. Do HQ and Bui NL, 'Discussing Personal Data Protection During Arbitration Proceedings and Lessons for Vietnam' (2024) 9(6) European Journal of Social Sciences Studies 75 <http://dx.doi.org/10.46827/ejsss.v9i6.1691> accessed 20 April 2026
10. Esposito M, Akbar Y and Campbell FX, *Digitalization in Emerging Economies* (CUP 2025)
11. González Pascual M, 'Public Administrations and Data Protection' in Sommermann KP, Krzywoń A and Fraenkel-Haeberle C (eds), *The Civil Service in Europe: A Research Companion* (Routledge 2025) 649 <http://dx.doi.org/10.4324/9781003458333-40> accessed 20 April 2026
12. Guamán DS and others, 'Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications' (2023) 130 Computers & Security 103262 <https://doi.org/10.1016/j.cose.2023.103262> accessed 20 April 2026
13. Ha HT and Vu TV, 'Potential Conflicts in Personal Data Protection under Current Legislation in Vietnam Compared with European General Data Protection Regulation' (2024) 7(3) Access to Justice in Eastern Europe 505 <https://doi.org/10.33327/ajee-18-7.3-a000304> accessed 20 April 2026

14. Hoofnagle CJ, van der Sloot B and Borgesius FZ, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28(1) Information & Communications Technology Law 65 <https://doi.org/10.1080/13600834.2019.1573501> accessed 20 April 2026

15. Hu G and others, 'The Influence of Public Engaging Intention on Value Co-Creation of E-Government Services' (2019) 7 IEEE Access 111145 <https://doi.org/10.1109/ACCESS.2019.2934138> accessed 20 April 2026

16. Huynh TT, 'Everyone is Safe Now: Constructing the Meaning of Data Privacy Regulation in Vietnam' (2024) 11(4) Asian Journal of Law and Society 530 <https://doi.org/10.1017/als.2024.36> accessed 20 April 2026

17. Iriye R, 'The European Union General Data Protection Regulation' (*Stimson Center*, 24 September 2024) <https://www.stimson.org/2024/the-european-union-general-data-protection-regulation/> accessed 20 April 2026

18. Jagannadh ML and Sumitra S, 'Comparative Analysis of Data Protection and Privacy Laws' (2025) 23(s6) Lex Localis – Journal of Local Self-Government 8565 <https://doi.org/10.52152/51h4tr43> accessed 20 April 2026

19. Janssen M and others, 'Trustworthiness of Digital Government Services: Deriving a Comprehensive Theory Through Interpretive Structural Modelling' (2018) 20(5) Public Management Review 647 <https://doi.org/10.1080/14719037.2017.1305689> accessed 20 April 2026

20. Joshi PR and Islam S, 'E-Government Maturity Model for Sustainable E-Government Services from the Perspective of Developing Countries' (2018) 10(6) Sustainability 1882 <https://doi.org/10.3390/su10061882> accessed 20 April 2026

21. Jurczuk M and Suprunowicz M, 'Consent in Data Privacy: A General Comparison of GDPR and HIPAA' (2024) 16 Przegląd Prawniczy Uniwersytetu Im Adama Mickiewicza 173 <https://doi.org/10.14746/ppuam.2024.16.07> accessed 20 April 2026

22. Kawintiranon K and Liu Y, 'Towards Automatic Comparison of Data Privacy Documents: A Preliminary Experiment on GDPR-Like Laws' (*arXiv*, 1 May 2021) arXiv:2105.10117 [cs.CL] <https://doi.org/10.48550/arXiv.2105.10117> accessed 20 April 2026

23. Kim SK, Park MJ and Rho JJ, 'Does Public Service Delivery Through New Channels Promote Citizen Trust in Government? The Case of Smart Devices' (2019) 25(3) Information Technology for Development 604 <https://doi.org/10.1080/02681102.2017.1412291> accessed 20 April 2026

24. Kuner C, 'Protecting EU Data Outside EU Borders under the GDPR' (2023) 60(1) Common Market Law Review 77 <https://doi.org/10.54648/cola2023004> accessed 20 April 2026

25. Le CTQ, Tran VD and Nguyen DPT, 'Global Norms and Regional Innovation: GDPR, Evolution of Data Protection in ASEAN and the Legal Trajectory of AI in Vietnam' (2025) 15(3) TalTech Journal of European Studies 250 <https://doi.org/10.2478/bjes-2025-0039> accessed 20 April 2026

26. Le VC, Nguyen XQ and Ngo KT, 'Processing of Children's Personal Data: A Comparative Study of the EU Legal Framework and Vietnamese Law' (2025) 15(2) TalTech Journal of European Studies 56 <https://doi.org/10.2478/bjes-2025-0020> accessed 20 April 2026

27. Ma L and Zheng Y, 'National E-Government Performance and Citizen Satisfaction: A Multilevel Analysis Across European Countries' (2019) 85(3) International Review of Administrative Sciences 506 <https://doi.org/10.1177/0020852317703691> accessed 20 April 2026

28. Nam GD and Khoi TD, 'More than Just Privacy: Latent Policies for the Codification of Vietnamese Personal Data Protection Law' (2025) 15(3) International Data Privacy Law 268 <https://doi.org/10.1093/idpl/ipaf013> accessed 20 April 2026

29. Nannini L and others, 'Beyond Phase-In: Assessing Impacts on Disinformation of the EU Digital Services Act' (2024) 5(2) AI and Ethics 1241 <https://doi.org/10.1007/s43681-024-00467-w> accessed 20 April 2026

30. Nguyen HBH, 'Addressing Fragmentation in Vietnam's Data Protection Laws: Recommendations for a Unified Legal Framework' (2024) 11(2) Vietnamese Journal of Legal Sciences 14 <https://doi.org/10.2478/vjls-2024-0008> accessed 20 April 2026

31. Pencheva I, Esteve M and Mikhaylov SJ, 'Big Data and AI – A Transformational Shift for Government: So, What Next for Research?' (2020) 35(1) Public Policy and Administration 24 <https://doi.org/10.1177/0952076718780537> accessed 20 April 2026

32. Rosenberg D, 'Use of E-Government Services in a Deeply Divided Society: A Test and an Extension of the Social Inequality Hypotheses' (2019) 21(2) New Media & Society 464 <https://doi.org/10.1177/1461444818799632> accessed 20 April 2026

33. Ryngaert C and Taylor M, 'The GDPR as Global Data Protection Regulation?' (2020) 114 American Journal of International Law 5 <https://doi.org/10.1017/aju.2019.80> accessed 20 April 2026

34. Samuel G, *An Introduction to Comparative Law Theory and Method* (Bloomsbury Publishing 2014)

35. Sirur S, Nurse JRC and Webb H, 'Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)' (*arXiv*, 22 August 2018) arXiv:1808.07338 [cs.CY] <https://doi.org/10.48550/arXiv.1808.07338> accessed 20 April 2026

36. Streinz T, 'The Evolution of European Data Law' in Craig P and de Búrca G (eds), *The Evolution of EU Law* (3rd edn, OUP 2021) 902 <https://doi.org/10.1093/oso/9780192846556.003.0029> accessed 20 April 2026

37. Thai TTD, Nguyen VD and Nguyen VL, 'A Comparative Study of Cross-Border Data Transfer Regulations in Vietnam and Singapore Ensuring the Protection of Privacy' (2025) 26(2) Asia-Pacific Journal on Human Rights and the Law 81 <https://doi.org/10.1163/15718158-26020001> accessed 20 April 2026

38. Tikkinen-Piri C, Rohunen A and Markkula J, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies' (2017) 34(1) Computer Law & Security Review 134 <https://doi.org/10.1016/j.clsr.2017.05.015> accessed 20 April 2026

39. To TL, 'Some Legal Aspects of Personal Data Protection in the World: Experience for Vietnam' (2024) 10(1) Cogent Social Sciences 2414872 <https://doi.org/10.1080/23311886.2024.2414872> accessed 20 April 2026

40. Tong TPT, 'Laws on Personal Data Protection in Vietnam Today' (2025) 14(1) International Journal of Engineering Inventions 47 <https://www.ijeijournal.com/v14-i1.html> accessed 20 April 2026

41. Voigt P and von Dem Bussche A, 'Practical Implementation of the Requirements under the GDPR' in Voigt P and von Dem Bussche A, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 245 <https://doi.org/10.1007/978-3-319-57959-7_10> accessed 20 April 2026

42. Ziemba EW, 'The Contribution of ICT Adoption to the Sustainable Information Society' (2019) 59(2) Journal of Computer Information Systems 116 <https://doi.org/10.1080/08874417.2017.1312635> accessed 20 April 2026

AUTHORS INFORMATION

Nguyen Thi Thuy
Faculty of Administrative and State Law, Hanoi Law University, Vietnam
nguyenthuy@hlu.edu.vn
https://orcid.org/0009-0003-2759-0960
Co-author, responsible for Conceptualization; Data curation; Software; Writing – original draft.

Tran Kim Lieu*
Law Clinic, Hanoi Law University, Vietnam
lieutk@hlu.edu.vn
https://orcid.org/0009-0008-7896-1369
Corresponding author, Data curation; Formal Analysis; Methodology; Project administration; Resources; Supervision; Writing – review & editing.

Vu Van Tuan
Faculty of Legal Foreign Languages, Hanoi Law University, Vietnam
tuanvv@hlu.edu.vn
https://orcid.org/0000-0002-3066-7338
Co-author, responsible for Validation; Visualization; Writing – review & editing.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that the opinion and views expressed in this manuscript are free of any impact of any organizations.

FUNDING STATEMENT

The authors received no specific grant or external funding for the research and publication of this article. Consequently, the Article Processing Charge (APC) was partially waived (50%) by the publisher in accordance with the AJEE Charges Policy for eligible countries (as per the IMF classification at the time of submission). The remaining balance was covered by the authors.

RIGHTS AND PERMISSIONS

EDITORS

ABOUT THIS ARTICLE

Cite this article
Nguyen TT, Lieu TK and Vu VT, 'Personal Data Protection in Vietnam's Public Administration: A Comparative Analysis with the EU General Data Protection Regulation' (2026) 9(4) Access to Justice in Eastern Europe <https://doi.org/10.33327/AJEE-18-9.4-a0002011>

DOI: https://doi.org/10.33327/AJEE-18-9.4-a0002011

***Keywords*:** *Administrative Law; Data Governance; Digital Governance; Legal Harmonization; Personal Data Protection.*

DETAILS FOR PUBLICATION

Date of submission: 18 Jun 2026
Date of acceptance: 03 Aug 2026
Online First Publication: 26 Sep 2026
Publication: Nov 2026
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 1 round with minor revisions

Technical tools were used in the editorial process

Plagiarism checks - Turnitin from iThenticate
https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review
https://scholasticahq.com/law-reviews
Paperpal for Academic Editing & Proofreading
https://paperpal.com/

AI DISCLOSURE STATEMENT

The authors acknowledge the use of Grammarly to improve language clarity and grammar. While the authors acknowledge the usage of AI, they maintain that they are the sole authors of this article and take full responsibility for the content therein, as outlined in COPE recommendations.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ПУБЛІЧНІЙ АДМІНІСТРАЦІЇ В'ЄТНАМУ: ПОРІВНЯЛЬНИЙ АНАЛІЗ ІЗ ЗАГАЛЬНИМ РЕГЛАМЕНТОМ ЄС ПРО ЗАХИСТ ДАНИХ

Нгуєн Тхі Тхуй, Чан Кім Льєу* та Ву Ван Туан

АНОТАЦІЯ

Передумови. *Розширення масштабів врядування на основі даних актуалізувало проблему захисту персональних даних у сфері публічної адміністрації. Хоча сучасні режими захисту даних ґрунтуються на спільних засадах, їх функціонування в публічному секторі залишається неоднорідним. У цьому дослідженні проаналізовано, як GDPR та Закон В'єтнаму № 91/2025/QH15 регулюють обробку персональних даних органами публічної влади, а також які наслідки мають виявлені між ними розбіжності для інституційної підзвітності та прав фізичних осіб.*

Методи. *У межах дослідження оцінено нормативну архітектуру, інституційну відповідальність і механізми забезпечення відповідності (комплаєнсу) у двох правових системах. Поєднання систематичного порівняльно-правового аналізу первинних нормативно-правових актів із тематичним аналізом вторинних джерел уможливило як структурне зіставлення, так і контекстуальне тлумачення правових реалій обох юрисдикцій. Доктринальний аналіз виявляє формальні юридичні вимоги, тоді як висновки щодо правозастосування ґрунтуються на опрацюванні вторинних джерел і не позиціонуються як первинні емпіричні результати.*

Результати та висновки. *Результати засвідчують, що наявність розвиненої правової бази сама по собі не гарантує ефективного захисту. Обидві системи демонструють часткову конвергенцію загальних засад захисту даних, утім істотно різняться щодо обробки даних у публічному секторі, оцінки впливу, внутрішніх функцій комплаєнсу, незалежності наглядових органів і механізмів примусового виконання правових вимог. Відмінності в адміністративній спроможності, організаційній культурі, системі нагляду та стратегіях цифрового врядування, виявлені у вторинній літературі, здатні впливати на рівень дотримання встановлених вимог. Відтак, формальну конвергенцію не слід ототожнювати з інституційною або функціональною еквівалентністю. Доведено, що дієвий захист персональних даних у публічній адміністрації залежить від узгодженості законодавства, інституцій та управлінських практик. Контекстуально адаптована гармонізація, підкріплена дієвим наглядом і належною адміністративною спроможністю, є критично важливою для гарантування прав людини та підвищення довіри до публічного врядування, заснованого на даних.*

Ключові слова: *адміністративне право, управління даними, цифрове врядування, гармонізація законодавства, захист персональних даних.*

TÓM TẮT BẰNG TIẾNG VIỆT*

Bài báo nghiên cứu

BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG NỀN HÀNH CHÍNH CÔNG VIỆT NAM: PHÂN TÍCH SO SÁNH VỚI QUY ĐỊNH CHUNG VỀ BẢO VỆ DỮ LIỆU CỦA LIÊN MINH CHÂU ÂU (GDPR)

Nguyễn Thị Thuỷ, Trần Kim Liễu*, Vũ Văn Tuấn

TÓM TẮT

Bối cảnh: *Sự phát triển mạnh mẽ của quản trị dựa trên dữ liệu đặt ra yêu cầu ngày càng cao đối với việc bảo vệ dữ liệu cá nhân trong hoạt động hành chính công. Mặc dù các hệ thống pháp luật hiện đại về bảo vệ dữ liệu cá nhân có sự tương đồng nhất định về các nguyên tắc nền tảng, việc áp dụng các nguyên tắc này trong khu vực công vẫn có sự khác biệt đáng kể giữa các quốc gia và khu vực pháp lý. Nghiên cứu này phân tích cách thức Quy định chung về bảo vệ dữ liệu của Liên minh châu Âu (GDPR) và Luật số 91/2025/QH15 của Việt Nam điều chỉnh hoạt động xử lý dữ liệu cá nhân của các cơ quan công quyền, qua đó làm rõ những khác biệt giữa hai hệ thống và hệ quả của các khác biệt này đối với trách nhiệm giải trình của cơ quan nhà nước cũng như việc bảo đảm quyền của chủ thể dữ liệu.*

Phương pháp nghiên cứu: *Nghiên cứu tập trung đánh giá cấu trúc quy phạm, trách nhiệm của các chủ thể thể chế và cơ chế bảo đảm tuân thủ trong hai hệ thống pháp luật. Phương pháp nghiên cứu được sử dụng là sự kết hợp giữa phân tích pháp lý so sánh một cách có hệ thống đối với các văn bản pháp luật sơ cấp và phân tích theo chủ đề đối với các nguồn tài liệu thứ cấp, qua đó cho phép vừa so sánh cấu trúc pháp lý, vừa lý giải các quy định trong bối cảnh thể chế và quản trị cụ thể của từng hệ thống. Phân tích pháp lý quy phạm được sử dụng để xác định các yêu cầu pháp lý chính thức; trong khi đó, các nhận định liên quan đến thực tiễn thi hành được tổng hợp từ các công trình nghiên cứu và tài liệu thứ cấp hiện có, không được xem là kết quả nghiên cứu thực nghiệm độc lập của nghiên cứu này.*

Kết quả và kết luận: *Kết quả nghiên cứu cho thấy việc thiết lập một khuôn khổ pháp lý tương đối đầy đủ và chặt chẽ chưa phải là điều kiện đủ để bảo đảm hiệu quả bảo vệ dữ liệu cá nhân trên thực tế. Hai hệ thống pháp luật có sự hội tụ nhất định về các nguyên tắc chung của bảo vệ dữ liệu cá nhân, song vẫn tồn tại những khác biệt đáng kể trong các quy định và cơ chế liên quan đến xử lý dữ liệu cá nhân trong khu vực công, đánh giá tác động đối với việc bảo vệ dữ liệu, chức năng tuân thủ nội bộ, tính độc lập của cơ quan giám sát và cơ chế thực thi pháp luật. Các khác biệt về năng lực hành chính, văn hóa tổ chức, cơ chế giám sát và chiến lược quản trị số được ghi nhận trong các tài liệu thứ cấp có thể tác động đáng kể đến mức độ tuân*

* The publication metadata in Vietnamese is presented as submitted by the author.

thủ trên thực tế. Vì vậy, sự tương đồng về mặt quy phạm không đồng nghĩa với sự tương đương về thể chế hoặc hiệu quả vận hành. Nghiên cứu cho rằng việc bảo vệ dữ liệu cá nhân một cách thực chất trong nền hành chính công đòi hỏi sự gắn kết và đồng bộ giữa khuôn khổ pháp luật, thiết chế thực thi và thực tiễn quản trị. Việc hài hòa hóa pháp luật cần được thực hiện trên cơ sở tôn trọng đặc thù bối cảnh, đồng thời phải đi kèm với cơ chế giám sát hiệu quả và năng lực hành chính phù hợp nhằm bảo đảm quyền của cá nhân và củng cố niềm tin của xã hội đối với quản trị công dựa trên dữ liệu.

Từ khóa: *luật hành chính, quản trị dữ liệu, quản trị số, hài hòa hóa pháp luật, bảo vệ dữ liệu cá nhân.*