Strata Social and Humanities Studies, 2026, Vol. 4, No. 2, 91–107
E-ISSN: 2987-2537 | P-ISSN: 2987-3193
doi: 10.59631/sshs.v4i2.577
Advance Access publication October 31, 2026

STRATA
SOCIAL AND HUMANITIES STUDIES
journals.stratapersada.com/index.php/sshs

The Urgency of Establishing an Independent Supervisory Authority in Personal Data Protection: A Comparative Study of Indonesia and France

Klarisa Anugraeni[1], Achmad Miftah Farid[2]

[1*]*Universitas Muhammadiyah Surakarta, Indonesia.* klarisaanugraeni@gmail.com
[2]*Universitas Muhammadiyah Surakarta, Indonesia.* amf209@ums.ac.id

Article History	Submitted	Revised	Accepted
	2026-07-28	2026-08-29 & 2026-10-16	2026-10-23

Abstract

The enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) and Government Regulation No. 33 of 2026 has strengthened Indonesia's personal data protection framework while raising questions about the independence and effectiveness of external supervision. This study aims to comparatively analyze personal data protection supervision in Indonesia and France and to identify institutional principles for strengthening Indonesia's supervisory authority. Employing normative legal research with statutory, comparative, and conceptual approaches, it examines PDP Law, Government Regulation No. 33 of 2026, *Loi n° 2024–449 SREN*, the GDPR, and the CNIL framework through qualitative descriptive-analytical and comparative legal methods. The findings show that Indonesia's framework now provides compliance supervision and administrative sanctions, including fines of up to 2% of annual revenue, but places the external supervisory authority under the President pursuant to Article 58 of the PDP Law, risking conflict of interest in supervising public entities. The CNIL demonstrates institutional independence through pluralistic composition, protection from hierarchical intervention, separation of investigative and sanctioning functions, adversarial procedures, and judicial review. Based on this comparison, the study underscores the urgency of redesigning Indonesia's supervisory authority to ensure impartial and effective enforcement while remaining compatible with the national constitutional and administrative-law framework.

Keywords: *Commission nationale de l'informatique et des libertés*, comparative law, Indonesia, France, personal data protection authority.

© The Author(s) 2026. Published by CV. Strata Persada Academia.
This is an Open Access article distributed under the terms of the Creative Common Attribution 4.0 International (CC BY 4.0)

INTRODUCTION

The development of digital technology and the evolution of the global internet network have transformed personal data from mere individual information into a strategic resource (Bumbungan, 2025), where the massive scale of its collection and processing is directly proportional to the high potential for misuse and the privacy vulnerability of data subject (Kronivets & Tymoshenko, 2022). The increasing dependence on digital platform in public services, commerce, finance, and other sectors has further intensified the need for effective mechanisms to ensure the security and lawful processing of personal data (Yuan & Li, 2019). Within the framework of a rule of law state (Toule, 2022), personal data protection is not merely a technical necessity, but a guarantee of human rights that must be protected by the state (Quintais et al., 2023). As a form of constitutional commitment, Indonesia enacted Law Number 27 of 2022 on Personal Data Protection (PDP Law) as a comprehensive legal foundation for data governance (Lestari et al., 2024).

Although this umbrella regulation is available, the effectiveness of data protection enforcement remains constrained by the absence of an independent external supervisory authority. Thus far, the supervisory mechanism has primarily relied on Data Protection Officers (DPOs) appointed by individual data controllers, whose authority remains confined to internal organizational functions and does not include independent investigative or judicial authority (Ireland, 2024). The weakness of this self-supervisory structure is reflected in recurring data breaches across public and private sectors, including major incidents involving Tokopedia, BPJS Kesehatan, Bank Syariah Indonesia, passport data, and taxpayer identification data. This trend of data protection failure is recorded periodically (longitudinally), ranging from the e-commerce sector such as the leak of 91 million Tokopedia accounts (Soleh Hasan Wahid, 2023), the public health sector through the exposure of 279 million BPJS Kesehatan participant data (Budiono et al., 2024), to a series of post-PDP Law enactment incidents such as the hacking of 34 million passport data by "Bjorka" in 2022 (Fageh & Solikhawati, 2022), the ransomware attack on Bank Syariah Indonesia (BSI) that breached 15 million customer data, and the leak of 6 million NPWP data in September 2024 (Hamadou et al., 2024).

Those recurring cross-sectoral incidents indicate a structural gap between the existence of legal norms and their effective enforcement, particularly where internal compliance mechanisms operate without independent external oversight. This gap raises a fundamental legal question concerning the institutional design of personal data protection supervision: how can Indonesia establish an authority that is sufficiently independent from executive intervention while possessing effective enforcement powers? Addressing this question, this study contributes to the legal scholarship by developing an institutional model of an independent Personal Data Protection Authority (PDPA), informed by a comparative analysis of France's *Commission Nationale de l'Informatique et des Libertés* (hereinafter abbreviated as CNIL) (Georgiou & Lambrinoudakis, 2021).

In contrast to the law enforcement landscape in Indonesia, several developed countries have established digital risk mitigation systems through the establishment of independent supervisory authorities (Farid et al., 2025). In this study, France was proportionately selected as a comparative

jurisdiction based on three fundamental methodological considerations: (1) the similarity of the roots of the civil law legal tradition with Indonesia which ensures the harmony of the country's administrative legal structure and ease of institutional adaptation; (2) the institutional maturity of the CNIL as one of the most established personal data supervisory pioneers that is the main reference for the European Union's General Data Protection Regulation (GDPR) framework; and (3) the CNIL's status as an independent administrative body (*autorité administrative indépendante*) that has independent enforcement authority (Bougiakiotis, 2021). Operationally, CNIL is equipped with full authority to conduct periodic supervision, inspect electronic data control systems, conduct forensic investigations, and impose administrative sanctions independently. This strong institutional characteristic provides legal certainty and a much more objective and structured compliance enforcement process.

Various previous literature on personal data protection in Indonesia generally still focuses on normative aspects of the PDP Law, sectoral compliance analysis, or evaluation of internal operational instruments. For example, the studies from Rinjani & Firmansyah (2025) and Yuspin et al. (2023) limit their analysis to the macro-structural barriers of cyber administration laws and the weaknesses of digital banking sectoral regulations that rely too much on administrative sanctions. On the other hand, the research of Lestari et al. (2026) and Khair & Wiraguna (2025) focuses its micro-evaluation on the compliance of digital platform privacy policies as well as the technical constraints of implementing Data Protection Impact Assessment (DPIA) due to the absence of derivative rules. Meanwhile, Pratama & Pati (2021) examines the impact of the external supervisory vacuum that places the Data Protection Officer (DPO) in a vulnerable position without legal protection from management intervention. Collectively, the literature only places the absence of supervisory institutions as operational obstacles or sectoral compliance issues, without stepping into the formulation of the Constitutional Law architecture regarding its institutional design. This is where the scientific novelty of this research lies, which is to fill the academic gap by focusing on the urgency and institutional design of an independent Personal Data Protection Authority (PDPA) with quasi-judicial authority based on Presidential Regulation, through a comparative study with the CNIL model in France.

The legal problems examined in this article focus on how personal data protection supervision is regulated and implemented in Indonesia and France, and why the establishment of an independent supervisory authority is an urgent necessity within Indonesia's personal data protection system. Aligned with these research problems, this study aims to comparatively analyze the supervisory systems in both countries while evaluating the institutional urgency to formulate a recommended ideal model for an independent supervisory authority in Indonesia. Theoretically, this article contributes new academic insights into personal data protection law and comparative constitutional law. Conceptually, this study provides policymakers with an institutional blueprint and legal justification for developing implementing regulations, particularly a Presidential Regulation, concerning the authority, institutional structure, independence safeguards, and operational boundaries of an independent PDPA in Indonesia.

METHOD

This study employs normative legal research to examine the institutional design of personal data protection supervision in Indonesia and France. It focuses on legal norms, principles, and doctrines governing supervisory authority, institutional independence, administrative enforcement, and the relationship between internal compliance mechanisms and external regulatory oversight (Wardiono et al., 2026). The research uses three complementary approaches: the statutory approach, the comparative approach, and the conceptual approach (Fajar & Achmad, 2019). The statutory approach examines the relevant legal frameworks, particularly Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) and Government Regulation No. 33 of 2026 in Indonesia, as well as France's data protection legislation, including *Loi n° 2024–449 SREN* (*Loi visant à sécuriser et à réguler l'espace numérique*) and the European Union's General Data Protection Regulation (GDPR). The comparative approach examines the Indonesian and French frameworks through four analytical dimensions: (1) the legal basis and institutional position of the supervisory authority; (2) safeguards for institutional independence; (3) supervisory and administrative enforcement powers, including procedural safeguards and judicial review; and (4) the respective functions of internal Data Protection Officers (DPOs) and external supervisory authorities. France was selected because its established supervisory model, represented by the *Commission Nationale de l'Informatique et des Libertés* (CNIL), provides a relevant basis for examining how an independent administrative authority operates within a personal data protection framework. The conceptual approach is used to assess institutional independence, functional separation, administrative legality, and accountability, particularly in determining the extent to which elements of the French model may be adapted to Indonesia's constitutional and administrative-law context (Dimyati et al., 2021).

The legal materials consist of primary, secondary, and tertiary sources. Primary legal materials include the relevant Indonesian and French legislation, the GDPR, and pertinent regulatory or institutional decisions. Secondary materials comprise scholarly books, peer-reviewed journal articles, and legal analyses concerning data protection supervision and independent regulatory authorities, while tertiary materials are used to clarify relevant legal terminology and concepts. The materials are collected through library research and document analysis. They are then analyzed qualitatively using descriptive-analytical and comparative legal methods. The analysis first identifies the normative and institutional characteristics of each supervisory framework, then compares their functions and safeguards, and finally evaluates the legal transferability of relevant institutional principles to Indonesia. This process provides the basis for formulating recommendations on strengthening institutional independence, clarifying the division of responsibilities between internal compliance officers and the external supervisory authority, and ensuring that administrative enforcement remains consistent with the principles of legality, accountability, and judicial review.

RESULTS AND DISCUSSION

Comparative Framework of Personal Data Protection in Indonesia and France

The regulatory framework for personal data protection in Indonesia has developed significantly following the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law)

and the subsequent issuance of Government Regulation No. 33 of 2026 concerning the Implementation of Law No. 27 of 2022 (PP No. 33/2026). While the PDP Law establishes the fundamental rights, obligations, institutional framework, and administrative sanctions for personal data protection, PP No. 33/2026 provides more detailed mechanisms concerning data processing, the appointment of Data Protection Officers, supervisory procedures, administrative sanctions, and dispute resolution. Accordingly, the Indonesian framework can no longer be characterized simply by the absence of implementing regulations; rather, the central institutional issue concerns how the supervisory framework established by the PDP Law and operationalized through PP No. 33/2026 can ensure effective and sufficiently independent external oversight.

Within this framework, the term of "*…Pejabat atau Petugas yang melaksanakan fungsi Pelindungan Data Pribadi (PPDP)…*"(Article 53 Law Number 27 of 2022 Concerning Personal Data Protection, 2022), which corresponds to the Data Protection Officer (DPO) concept, functions primarily as an internal compliance mechanism. PP No. 33/2026 further regulates the PPDP in relation to the responsibilities of data controllers and processors, thereby strengthening the organizational dimension of personal data protection compliance. However, an internal compliance officer and an external supervisory authority perform different institutional functions. The PPDP is responsible for facilitating compliance within the organization, whereas an external supervisory authority is required to exercise oversight over controllers and processors, conduct supervisory activities, and impose administrative sanctions where legally authorized. This distinction is important because strengthening internal compliance does not, by itself, eliminate the need for an institution capable of exercising external and impartial supervision.

The Indonesian framework also now provides a more concrete basis for external supervision. PP No. 33/2026 contains a specific chapter on supervision of the compliance of data controllers and processors and regulates administrative sanctions, including written warnings, temporary suspension of data processing, deletion or destruction of personal data, and administrative fines (Government Regulation Number 33 of 2026 Concerning Instruction Code of Law Number 27 of 2022 Concerning Personal Data Protection, 2026). The regulation further provides that administrative sanctions are imposed by the institution responsible for personal data protection, with administrative fines potentially reaching 2% of the annual revenue or income of the relevant controller or processor, subject to the variables and procedures prescribed by the regulation. Thus, the principal legal problem has shifted from whether Indonesia possesses an operational framework for supervision to whether the institution entrusted with these powers is designed with adequate independence, accountability, and institutional safeguards (Haliwela, 2023).

France provides a useful comparative reference through the CNIL, established under *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. Currently, the regulation has been replaced and strengthened under the umbrella law of *Loi n° 2024–449 SREN* (*Loi visant à sécuriser et à réguler l'espace numérique*). In contrast to a supervisory architecture that relies principally on internal organizational compliance, the French model combines internal compliance mechanisms with an external independent administrative authority (Clément-fontaine, 2024). The CNIL has supervisory and enforcement functions, including receiving complaints, conducting investigations, and imposing administrative sanctions (Maskun &

Nugraha, 2020). The institutional significance of this model lies not merely in the existence of a supervisory authority, but in the separation between the organization's internal compliance function and the state's external supervisory function.

The comparison therefore reveals that the principal institutional issue is the relationship between internal compliance and external supervision. Indonesia's PPDP mechanism and France's DPO mechanism may serve comparable internal compliance functions, but the French system demonstrates the importance of placing an external supervisory authority in a position institutionally distinct from the entities that it supervises (Patureau, 2026). This distinction is particularly relevant in Indonesia because public bodies are themselves subject to personal data protection obligations. An effective supervisory institution must therefore be capable of exercising its statutory functions not only toward private entities but also toward public-sector data controllers without being subject to inappropriate executive intervention (Clément-fontaine, 2024).

This comparison highlights the fundamental weakness of Article 58 of the PDP Law, which places the supervisory agency under and accountable to the President. This construction of executive subordination has the potential to trigger a conflict of interest when supervising government entities, in contrast to the CNIL, which has power across ministries.

Table 1. Comparative Framework of Personal Data Protection Supervision between Indonesia and France

No	Dimension	Indonesian Supervisory Authority (Based on PP 27/2022)	French Authority (CNIL)
1	Primary Legal Basis	Law No. 27 of 2022 and Government Regulation (PP) No. 33 of 2026	*Loi n° 2024–449 SREN* (*Loi visant à sécuriser et à réguler l'espace numérique*)
2	Internal compliance mechanism	PPDP/DPO within data controllers and processors	DPO/internal compliance within organizations
3	External supervisory authority	Institution responsible for personal data protection as contemplated by the PDP Law (Article 58) and operationalized through the implementing framework	CNIL as an independent administrative authority
4	Supervisory function	PP No. 33/2026 regulates external supervision of compliance and related procedures, projected to be effective in January 2027	CNIL exercises external supervisory, investigative, complaint-handling, and enforcement functions

5	Administrative sanctions	Written warning, temporary suspension, deletion/destruction, and administrative fines up to 2% of annual revenue or income under the prescribed conditions	Administrative enforcement and sanctions exercised by CNIL within its statutory competence
6	Relationship between DPO and external authority	PPDP functions as an internal compliance mechanism; external supervision remains institutionally distinct	DPO performs internal compliance functions, while CNIL performs external regulatory supervision
7	Institutional independence	The principal issue concerns the institutional design and independence of the authority exercising the statutory supervisory mandate	Institutional independence is expressly embedded in the legal status of CNIL

Table 1 demonstrates that Indonesia and France share a two-level logic of personal data protection: internal organizational compliance and external regulatory supervision. The significant difference lies in the maturity and institutional positioning of the external supervisory authority. PP No. 33/2026 has substantially strengthened Indonesia's regulatory and procedural framework, including the mechanisms for supervision and administrative sanctions, but the effectiveness of these mechanisms ultimately depends on the institutional capacity and independence of the authority entrusted with their implementation (Pane et al., 2026).

Consequently, the French CNIL should not be transplanted mechanically into the Indonesian legal system. The relevant comparative lesson is instead functional: effective personal data protection requires a clear institutional separation between internal compliance officers and an external supervisory authority, together with legally defined supervisory and enforcement powers (Choe, 2025). The Indonesian institutional model should therefore build upon the framework already established by the PDP Law and PP No. 33/2026 while addressing the remaining question of how institutional independence, accountability, and the limits of administrative enforcement should be designed within Indonesia's constitutional and administrative-law structure.

Institutional Independence and Enforcement: Lessons from CNIL for Indonesia

The comparative analysis demonstrates that the principal challenge for Indonesia is no longer the absence of a regulatory framework for personal data protection. With the enactment of PP No. 33 of 2026, the implementation of Law No. 27 of 2022 has been further operationalized through detailed provisions concerning compliance supervision and administrative sanctions. The

regulation authorizes the institution responsible for personal data protection (the "Institution") to conduct monitoring, control, examination, and investigation of alleged violations and to impose administrative sanctions on data controllers and processors (Supriyadi, 2023). These sanctions include written warnings, temporary suspension of data processing, deletion or destruction of personal data, and administrative fines of up to 2% of the controller's or processor's annual revenue or income (Article 185 Government Regulation Number 33 of 2026 Concerning Instruction Code of Law Number 27 of 2022 Concerning Personal Data Protection, 2026). The remaining institutional question is therefore not whether Indonesia has supervisory powers in normative terms, but whether the institution exercising those powers possesses sufficient independence and procedural safeguards to perform its functions effectively and impartially.

This issue becomes particularly significant because the supervisory authority operates in a regulatory environment in which public institutions themselves may act as data controllers. The effectiveness of external supervision consequently depends upon the ability of the supervisory institution to examine both private and public entities without inappropriate interference from the institutions being supervised (Dove & Chen, 2021). Independence in this context should not be understood as complete institutional detachment from the state. Rather, it refers to the capacity of the supervisory authority to exercise its statutory functions without hierarchical direction from the entities whose compliance it is mandated to supervise, while remaining subject to legal accountability, procedural safeguards, and judicial review (Möller, 2026).

The French CNIL provides a relevant institutional reference in this regard. The CNIL is expressly established as an independent administrative authority under the French data protection framework (Becker, 2018). Its institutional composition also reflects a pluralistic design: the Commission consists of 18 members, including representatives of the judiciary, Parliament, the Economic, Social and Environmental Council, and qualified persons (Nicolas-Vullierme, 2020). The CNIL itself emphasizes that ministers, public authorities, and private entities cannot oppose its actions, while its chair has authority to recruit its staff. This institutional configuration illustrates that regulatory independence is not merely a declaration of organizational autonomy, but can be constructed through appointment mechanisms, collegial composition, personnel arrangements, and protection from hierarchical intervention (Lorange, 2021).

The CNIL's enforcement model further demonstrates the importance of combining regulatory independence with procedural constraints. The authority possesses powers of investigation and sanction, but these powers are not exercised without legal limitations. In particular, the French framework separates the functions of initiating enforcement proceedings from the imposition of sanctions through its internal institutional structure. The President of the CNIL may refer a matter to the restricted formation, which then determines the appropriate sanction following an adversarial procedure. French administrative jurisprudence also emphasizes that sanctioning powers entrusted to independent administrative authorities must respect the rights of defence, adversarial proceedings, independence, and impartiality, while sanctions remain subject to judicial review (Y. Lestari & Mujib, 2022). The significance of the French model therefore lies not simply in granting an independent authority the power to impose

fines, but in coupling enforcement authority with institutional and procedural safeguards (Natamiharja & Setiawan, 2024).

This point is particularly relevant to the Indonesian framework following PP No. 33 of 2026. The regulation already provides the legal mechanism for administrative supervision and sanctions, including a maximum administrative fine of 2% of annual revenue or income. Therefore, reproducing the 2% sanction as a new institutional proposal would add little analytical value (Article 185 Government Regulation Number 33 of 2026 Concerning Instruction Code of Law Number 27 of 2022 Concerning Personal Data Protection, 2026). The more important question is how the authority entrusted with imposing such a substantial sanction should be structured so that the exercise of coercive administrative power remains lawful, impartial, proportionate, and reviewable. In other words, the institutional design should precede the discussion of the magnitude of sanctions.

The comparative lesson also requires a distinction between administrative enforcement and judicial adjudication. The CNIL demonstrates that an independent administrative authority may possess significant enforcement powers without thereby becoming part of the judicial branch. Its sanctions remain administrative in character and are subject to judicial review (Natamiharja & Setiawan, 2024). Accordingly, the proposed Indonesian institution should not be conceptualized as a substitute for the courts or as an institution possessing unrestricted quasi-judicial authority. Its primary role should be administrative supervision, investigation, compliance enforcement, and the imposition of administrative sanctions within powers expressly provided by law. Where the exercise of coercive authority affects fundamental rights or where a sanction is challenged, judicial review provides the necessary external guarantee against arbitrary administrative action (Farid et al., 2025).

From this perspective, the establishment of an independent Personal Data Protection Authority (PDPA) in Indonesia should be understood as an institutional strengthening of the supervisory framework already established by the PDP Law and PP No. 33 of 2026, rather than as the creation of an entirely new regulatory regime. The PDPA would occupy the external supervisory level, while PPDPs/DPOs would remain internal compliance officers within data controllers and processors (Widiatedja & Mishra, 2023). The two institutions should therefore operate through functional complementarity: PPDPs facilitate organizational compliance, whereas the PDPA conducts external supervision, receives complaints, undertakes investigations, and exercises administrative enforcement in accordance with statutory authority (Shalihah & Mohd Shariff, 2022).

However, the French model cannot be transplanted mechanically into the Indonesian legal system. France's institutional architecture developed within a different constitutional and administrative framework, including its established category of independent administrative authorities. The Indonesian model must instead identify the functional elements that are compatible with its own legal order. These elements include institutional independence from the entities being supervised, pluralistic and transparent appointment procedures, security of tenure, adequate organizational capacity, clear separation between investigative and sanctioning

functions, procedural protection for regulated entities and data subjects, and access to judicial review (Kronivets & Tymoshenko, 2022).

Accordingly, the principal contribution of the CNIL comparison is not the proposition that Indonesia should reproduce the French authority in identical form. Rather, it demonstrates a functional relationship between institutional independence, effective supervision, and legitimate enforcement. PP No. 33 of 2026 has filled an important regulatory gap by operationalizing supervision and administrative sanctions, but the effectiveness of these provisions depends upon the institutional characteristics of the authority that will implement them. The Indonesian reform agenda should therefore focus on ensuring that the Lembaga established under the PDP framework possesses sufficient independence, accountability, and procedural safeguards to supervise both public and private data controllers effectively, while maintaining judicial review as a safeguard against excessive administrative power.

Institutional Complementarity between Internal Compliance and External Supervision

The preceding analysis indicates that an effective personal data protection system requires a clear distinction between internal compliance and external regulatory supervision (Dewi, 2018). Although both functions contribute to the protection of data subjects' rights, they operate at different institutional levels and serve different purposes. Internal compliance mechanisms assist data controllers and processors in fulfilling their legal obligations, whereas an external supervisory authority independently assesses compliance, investigates alleged violations, and exercises enforcement powers within the limits established by law (Setyoningsih & Farid, 2025). Accordingly, strengthening personal data protection in Indonesia should not be understood as a choice between improving the role of Data Protection Officers (DPOs) and establishing an effective external supervisory authority. Both mechanisms are necessary, but their respective mandates must remain clearly differentiated (Rudolf & Kovač, 2026).

The French framework illustrates this distinction. Under the General Data Protection Regulation (GDPR), a DPO informs and advises the organization that appoints the officer, monitors compliance, and cooperates with the supervisory authority. The DPO must be able to perform these duties independently within the organization and must not receive instructions concerning the exercise of the DPO's assigned tasks (Pratama & Pati, 2021). Nevertheless, this internal independence does not transform the DPO into a public supervisory authority. The controller or processor remains responsible for compliance with data protection law, while the CNIL retains its distinct regulatory and enforcement functions. The CNIL's guidance further emphasizes that DPOs must receive adequate resources and occupy an organizational position that enables them to perform their duties effectively (Dalmat, 2025).

This distinction has direct implications for the implementation of Indonesia's PDP Law and Government Regulation No. 33 of 2026. The regulatory framework should be understood as comprising two complementary institutional functions: organizational compliance through the PPDP and external supervision by the institution entrusted with supervisory powers under the personal data protection framework. The PPDP should facilitate compliance, provide internal advice, identify potential risks, and communicate data protection concerns to the organization's management. The external authority, by contrast, should supervise data controllers and

processors, assess complaints, conduct examinations or investigations within its lawful competence, and impose administrative sanctions where the applicable legislation authorizes it to do so (Badar et al., 2023).

A potential institutional problem arises if the relationship between the PPDP and the external authority is designed as a hierarchical reporting arrangement. Requiring PPDPs to report routinely to the external authority as if they were subordinate officials could blur the distinction between internal compliance and public supervision. It could also create uncertainty regarding the PPDP's professional responsibilities, particularly when the officer must advise the organization against a proposed data processing activity. The GDPR framework offers a more appropriate functional reference: the DPO reports to the highest level of management within the organization and cooperates with the supervisory authority in accordance with applicable legal obligations. The DPO's role is therefore not to act as an extension of the regulator, but to facilitate compliance while maintaining sufficient professional independence within the organization (Georgiou & Lambrinoudakis, 2021).

For Indonesia, the relationship between the PPDP and the external supervisory authority should consequently be based on functional cooperation rather than administrative subordination. The external authority may issue guidance, develop compliance standards, provide training, and establish procedures through which organizations can demonstrate compliance (Feretzakis et al., 2025). PPDPs may serve as institutional contact points where the law requires communication with the supervisory authority. However, any reporting obligation, disclosure of information, or duty to cooperate must be grounded in applicable law and accompanied by appropriate safeguards for confidentiality, data subjects' rights, and the legitimate interests of the organization. This approach would preserve the internal compliance function while enabling the supervisory authority to obtain the information necessary to carry out its statutory mandate (Badar et al., 2023).

The institutional model should also distinguish between the responsibilities of the organization, the functions of the PPDP, and the enforcement powers of the supervisory authority. First, data controllers and processors remain legally responsible for ensuring that their processing activities comply with personal data protection requirements. Second, PPDPs assist and monitor compliance internally but do not assume the organization's ultimate legal responsibility. Third, the external supervisory authority exercises public powers independently within the limits of its legal mandate (Díaz Díaz, 2016). This allocation of responsibilities helps avoid a situation in which an organization treats the appointment of a PPDP as sufficient evidence of compliance or attempts to transfer its legal responsibility to the officer. It also prevents the external authority from becoming overly dependent on internal officers to initiate or substantiate enforcement action (Nag et al., 2022).

Based on these considerations, the institutional reform proposed in this study should focus on strengthening the external supervisory function while preserving the distinct role of internal compliance officers. The relevant institutional safeguards include transparent appointment procedures, protection against inappropriate executive intervention, adequate human and financial resources, clearly defined supervisory and sanctioning powers, impartial decision-

making procedures, and access to judicial review. The French experience demonstrates the importance of combining regulatory independence with procedural accountability; however, the precise institutional arrangements must be adapted to Indonesia's constitutional structure and statutory framework rather than copied directly from the French system (Nicolas-Vullierme, 2020).

The proposed model therefore rests on three mutually reinforcing principles: institutional independence, functional separation, and legal accountability. Institutional independence enables the external authority to supervise both public and private data controllers without inappropriate interference (Lamchek, 2023). Functional separation ensures that PPDPs remain internal compliance officers rather than subordinate agents of the state supervisory authority. Legal accountability requires that supervisory and sanctioning powers have a sufficient legal basis, follow fair procedures, and remain subject to judicial review (Farid & Prasetyoningsih, 2023). Together, these principles provide a more legally defensible approach to strengthening Indonesia's personal data protection framework following the enactment of PP No. 33 of 2026. Rather than creating overlapping supervisory structures, the proposed reform seeks to establish a coherent relationship between organizational compliance and independent external enforcement, thereby improving the institutional protection of data subjects' rights (Rudolf & Kovač, 2026).

CONCLUSION

This comparative study finds that Indonesia's personal data protection framework has advanced substantially through Law No. 27 of 2022 and Government Regulation No. 33 of 2026, which operationalise compliance supervision mechanisms, administrative sanctions (including fines of up to 2 percent of annual revenue or income), and the role of the Personal Data Protection Officer (PPDP) as an internal compliance mechanism. Nevertheless, the principal finding is that the effectiveness of this framework remains constrained by the institutional design of the external supervisory authority, which is placed under and accountable to the President (Article 58 of the PDP Law). This arrangement risks creating conflicts of interest, particularly when the authority supervises public-sector entities. By contrast, the French model, embodied in the Commission Nationale de l'Informatique et des Libertés (CNIL) as an independent administrative authority, demonstrates the importance of a clear institutional separation between internal compliance functions (performed by the Data Protection Officer) and external supervision. This separation is reinforced by institutional independence, pluralistic composition, protection from hierarchical intervention, adversarial procedures, and judicial review. Theoretically, these findings enrich the discourse on administrative law and regulatory governance by showing that supervisory independence is not merely a formal declaration of organisational autonomy, but a carefully constructed institutional arrangement that enables impartial oversight of both private and public actors while remaining subject to legal accountability. Practically, the results underscore the urgency of strengthening the institutional design of Indonesia's Personal Data Protection Authority so that it can exercise supervisory, investigative, and sanctioning powers effectively, proportionately, and free from undue executive interference, thereby enhancing the protection of data subjects' rights.

This study is limited by its doctrinal and normative comparative approach, which does not include in-depth empirical analysis of the actual implementation of Government Regulation No. 33 of 2026 (fully effective only in 2027) or a detailed evaluation of the CNIL's day-to-day operational performance. Moreover, differences in constitutional systems and administrative-law traditions between Indonesia and France restrict direct generalisation. Future research should therefore examine empirically the institutional capacity, accountability mechanisms, and practical effects of administrative sanctions in Indonesia following full implementation, while also exploring hybrid models compatible with Indonesia's constitutional and administrative-law framework. Institutional reform should prioritise enhanced independence, transparent appointment procedures, a clear separation between investigative and sanctioning functions, and guaranteed access to judicial review. Rather than mechanically transplanting the CNIL model, Indonesia should adapt the functional elements that prove relevant, thereby establishing a coherent relationship between internal organisational compliance and effective external supervision.

REFERENCES

Badar, E. S., Fauzi, A., & Jazuli, A. (2023). Personal Data Protection Policy in Law Number 27 of 2022 in the Perspective of Positive Law and Islamic Law. *Hukum Islam*, *23*(1), 61–74. https://doi.org/10.24014/jhi.v23i1.20465

Becker, M. (2018). Ethics in the big data era: Privacy as autonomy and privacy as dignity | Ethiek in het big data tijdperk. Privacy als autonomie en als waardigheid. *Tydskrif Vir Geesteswetenskappe*, *58*(4), 669–682. https://doi.org/10.17159/2224-7912/2018/v58n4-la4

Bougiakiotis, E. (2021). One law to rule them all? The reach of EU data protection law after the Google v CNIL case. *Computer Law & Security Review*, *42*, 105580. https://doi.org/https://doi.org/10.1016/j.clsr.2021.105580

Budiono, A., Nurrizky, A. S., Fairuzzaman, F., Gulyamov, S. S., Prakoso, A. L., Yuspin, W., Farid, A. M., & Ogli, T. M. A. P. (2024). Lesson From Indonesia National Healthcare Security (BPJS Kesehatan): HIV/AIDS Patient Medical Data Protection Policies. *Malaysian Journal of Medicine and Health Sciences*, *20*, 201–208. https://doi.org/10.47836/mjmhs.20.s9.33

Bumbungan, S. (2025). Peran dan Perkembangan Jaringan Internet dalam Mendukung Transformasi Digital Global. *Bulletin of Network Engineer and Informatics*, *3*(1), 11–15. https://doi.org/10.59688/bufnets.v3i1.66

Choe, H. J. (2025). The EU AI Act Based on the Precautionary Principle and France's Response: Focused on the Protection of the Right to One's Image. *Journal of Intellectual Property*, *20*(4), 147–163. https://doi.org/10.34122/jip.2025.20.4.147

Clément-fontaine, M. (2024). French law to secure and regulate the digital space and European digital law. *Revue Lamy Droit de l'immatériel*, *X*. https://hal.science/hal-04822544

Dalmat, Y.-M. (2025). La CNIL alerte sur les ingérences étrangères dans nos trafics numériques. *Option/Bio*, *37*(723–724), 13. https://doi.org/10.1016/S0992-5945(26)75004-2

Dewi, S. (2018). Privacy: An overview of Indonesia Statutes Governing lawful interception. *Central European Journal of International and Security Studies*, *12*(4), 587–597.

https://cejiss.org/privacy-an-overview-of-indonesia-statutes-governing-lawful-interception

Díaz Díaz, E. (2016). The new European Union General Regulation on Data Protection and the legal consequences for institutions. *Church, Communication and Culture*, *1*(1), 206–239. https://doi.org/10.1080/23753234.2016.1240912

Dimyati, K., Nashir, H., Elviandri, E., Absori, A., Wardiono, K., & Budiono, A. (2021). Indonesia as a legal welfare state: A prophetic-transcendental basis. *Heliyon*, *7*(8), e07865. https://doi.org/10.1016/j.heliyon.2021.e07865

Dove, E. S., & Chen, J. (2021). What does it mean for a data subject to make their personal data "manifestly public"? An analysis of GDPR Article 9(2)(e). *International Data Privacy Law*, *11*(2), 107–124. https://doi.org/10.1093/idpl/ipab005

Fageh, A., & Solikhawati, A. (2022). The Bjorka Hacking Phenomenon on Selling Personal Data as a Digital Asset from The Perspective of Maqashid Sharia. *Jurnal Hukum Islam*, *20*(2), 279–298. https://doi.org/10.28918/jhi.v20i2.6387

Fajar, M., & Achmad, Y. (2019). *Dualisme Penelitian Hukum: Normatif dan Empiris* (5th ed.). Pustaka Pelajar.

Farid, A. M., & Prasetyoningsih, N. (2023). Legal Reasoning of the Constitutional Court Verdict Number 25/PUU-XX/2022 on the State Capital Law According to Social Justice Value. *Jurnal Jurisprudence*, *12*(2), 217–232. https://doi.org/10.23917/jurisprudence.v12i2.1285

Farid, A. M., Pratama, F. A., & Sulisyowati, D. (2025). Maqashid Sharia Analysis on Personal Data Protection from the Dangers of Artificial Intelligence Misuse. *Jurnal Penelitian Ilmu-Ilmu Sosial*, *6*(2), 179–192. https://doi.org/10.23917/sosial.v6i2.12636

Feretzakis, G., Vagena, E., Kalodanis, K., Peristera, P., Kalles, D., & Anastasiou, A. (2025). GDPR and Large Language Models: Technical and Legal Obstacles. *Future Internet*, *17*(4), 1–26. https://doi.org/10.3390/fi17040151

Georgiou, D., & Lambrinoudakis, C. (2021). Data protection impact assessment (DPIA) for cloud-based health organizations. *Future Internet*, *13*(3), 1–12. https://doi.org/10.3390/fi13030066

Haliwela, N. S. (2023). The Essence of Legal Protection of Personal Data of Customers In Banking Transactions. *SASI*, *29*(3), 548. https://doi.org/10.47268/sasi.v29i3.1528

Government Regulation Number 33 of 2026 concerning Instruction Code of Law Number 27 of 2022 concerning Personal Data Protection. (2026).

Hamadou, I., Yumna, A., Hamadou, H., & Jallow, M. S. (2024). Unleashing the power of artificial intelligence in Islamic banking: A case study of Bank Syariah Indonesia (BSI). *Modern Finance*, *2*(1), 131–144. https://doi.org/10.61351/mf.v2i1.116

Ireland, L. (2024). We are all (not) Anonymous: Individual- and country-level correlates of support for and opposition to hacktivism. *New Media & Society*, *26*(8), 4429–4453. https://doi.org/10.1177/14614448221122252

Khair, F., & Wiraguna, S. A. (2025). Data Protection Impact Assessment (DPIA) sebagai instrumen

kunci menjamin kepatuhan UU PDP 2022 di Indonesia. *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora*, *2*(2), 246–254. https://doi.org/10.62383/progres.v2i2.1821

Kronivets, T. M., & Tymoshenko, Y. A. (2022). Legal Aspects of Human Privacy Protection in the Context of the Use of Artificial Intelligence. *Juridical Scientific and Electronic Journal*, *12*, 295–297. https://doi.org/10.32782/2524-0374/2022-12/68

Lamchek, J. S. (2023). Ensuring Data Science and Its Applications Benefit Humanity: Data Monetization and the Right to Science. *Human Rights Law Review*, *23*(3), 1–23. https://doi.org/10.1093/hrlr/ngad018

Law Number 27 of 2022 concerning Personal Data Protection, Pub. L. No. 27 (2022).

Lestari, A. Y., Misran, Raharjo, T., Annas, M., Riskanita, D., & Prabandari, A. P. (2024). Improving Healthcare Patient Data Security: An Integrated Framework Model For Electronic Health Records From A Legal Perspective. *Law Reform: Jurnal Pembaharuan Hukum*, *20*(2), 329–352. https://doi.org/10.14710/lr.v20i2.56986

Lestari, C. R., Az'zahra, A. B., Octavia, N. M., Pandia, F. K. B. S., Wirdani, R., & Takhir, S. H. (2026). Analisis Tingkat Kepatuhan Pengelolaan Data Pribadi Pengguna terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) pada Platform Digital. *Adagium: Jurnal Ilmiah Hukum*, *4*(1), 146–168. https://doi.org/10.70308/adagium.v4i1.279

Lestari, Y., & Mujib, M. M. (2022). Optimizing Personal Data Protection Legal Framework in Indonesia (a Comparative Law Study). *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, *11*(2), 203–234. https://doi.org/10.14421/sh.v11i2.2729

Lorange, A. (2021). GDPR in France: A Lot of Communication for a Jurisdiction Well Experienced in the Protection of Personal Data. In E. Kiesow Cortez (Ed.), *Information Technology and Law Series* (pp. 59–81). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-407-5_4

Maskun, & Nugraha, R. (2020). The Practice of General Data Protection Regulations Fine and Penalty on Google Inc. vs CNIL Case. *International Journal of Law and Public Policy*, *2*(1), 1–7. https://doi.org/10.36079/lamintang.ijlapp-0201.85

Möller, K. (2026). Liberty and personal responsibility in Dworkin's theory of rights. *International Journal of Constitutional Law*, *24*(3), 787–814. https://doi.org/10.1093/icon/moag080

Nag, A. K., Bhadauria, V. S., Gibson, C., Neupane, R. C., & Creider, D. (2022). A Conceptual Learning Framework of Cybersecurity Education for Military and Law Enforcement. *International Journal of Smart Education and Urban Society*, *13*(1), 1–14. https://doi.org/10.4018/ijseus.309953

Natamiharja, R., & Setiawan, I. (2024). Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France. *Jambe Law Journal*, *7*(1), 233–251. https://doi.org/10.22437/home.v7i1.349

Nicolas-Vullierme, L. (2020). Data Protection in the Internet: French Report. In D. Moura Vicente & S. de Vasconcelos Casimiro (Eds.), *Ius Comparatum - Global Studies in Comparative Law* (pp. 159–181). Springer International Publishing. https://doi.org/10.1007/978-3-030-28049-9_6

Pane, M. D., Maryati, M., & Setiyadi, A. (2026). Encryption , Digital Governance , and Personal

Data Protection : Developing a Juridical – Technical Enforcement Model under Indonesia ' s Law No . 27 of 2022. *Greenation International Journal of Law and Social Sciences*, *4*(4), 1375–1399. https://doi.org/10.38035/gijlss.v4i4.1080

Patureau, S. (2026). National development privacy protection tool found abusive: the apple case (France). *Journal of European Competition Law & Practice*, *17*(3), 149–152. https://doi.org/10.1093/jeclap/lpaf066

Pratama, A. M., & Pati, U. K. (2021). Analysis Principles of Personal Data Protection on COVID-19 Digital Contact Tracing Application: PeduliLindungi Case Study. *Lex Scientia Law Review*, *5*(2), 65–88. https://doi.org/10.15294/lesrev.v5i2.50601

Quintais, J. P., Appelman, N., & Fathaigh, R. (2023). Using Terms and Conditions to apply Fundamental Rights to Content Moderation. *German Law Journal*, *41*, 881–911. https://doi.org/10.1017/glj.2023.53

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83. https://doi.org/10.38043/jah.v8i1.6793

Rudolf, G., & Kovač, P. (2026). Who guards the guardians? Governing the independence and impartiality of data protection officers under the GDPR. *International Review of Law, Computers & Technology*, 1–27. https://doi.org/10.1080/13600869.2026.2705074

Setyoningsih, A. D. A., & Farid, A. M. (2025). Prophetic Cyber Law Enforcement: A Holistic Paradigm of Cyber Law Enforcement in Indonesia. *Proceedings of the 1st International Conference on Social Environment Diversity (ICOSEND 2024)*, *Icosend 2024*, 756–769. https://doi.org/10.2991/978-2-38476-366-5_76

Shalihah, F., & Mohd Shariff, R. N. (2022). Identifying Barriers To Data Protection and Investor Privacy in Equity Crowdfunding: Experiences From Indonesia and Malaysia. *UUM Journal of Legal Studies*, *13*(2), 215–242. https://doi.org/10.32890/uumjls2022.13.2.9

Soleh Hasan Wahid. (2023). Formulation of a Risk-Based Online Dispute Resolution Model for E-Commerce in Indonesia: Legal Framework and its Application. *International Journal of Arts and Humanities Studies*, *3*(2), 09–23. https://doi.org/10.32996/ijahs.2023.3.2.2

Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*, *3*(1), 33–69. https://doi.org/10.53955/jhcls.v3i1.71

Toule, E. R. M. (2022). Rule of Law and Rule of Ethic in Law Enforcement in Indonesia. *SASI*, *28*(1), 56. https://doi.org/10.47268/sasi.v28i1.752

Wardiono, K., Isman, I., Budiono, A., Yuspin, W., & Ken, D. (2026). Reconstruction of Legal Research Methodology : An Epistemological Review of the Prophetic Law. *Greenation International Journal of Law and Social Sciences*, *4*(4), 1265–1283. https://doi.org/https://doi.org/10.38035/gijlss.v4i4

Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: a future–forward perspective. *International Review of Law, Computers & Technology*, *37*(3), 252–273. https://doi.org/10.1080/13600869.2022.2155793

Yuan, B., & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Environmental Research and Public Health*, *16*(6), 1070. https://doi.org/10.3390/ijerph16061070

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1), 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130