PUBLIC SPHARE:
Jurnal Sosial Politik, Pemerintahan dan Hukum
ISSN (Online): 2964-5166
DOI: 10.59818/jps.v4i3.2317
Vol. 4, No. 3, November 2025

Strengthening the Functional Autonomy of Data Protection Officers Under Indonesia's PDP Law 2022: A Critical Legal and Institutional Review

Sidi Ahyar Wiraguna[1]
[1] Faculty of Law, Esa Unggul University, Jakarta-Indonesia
Email: *adipatiwiraguna@gmail.com*

RIWAYAT ARTIKEL
Received : 2025-11-20
Revised : 2025-11-26
Accepted : 2025-11-27

KEYWORDS
Data Capitalism; DPO Independence; Personal Data Protection; PDP Law 2022; PPDP

KATA KUNCI
Kapitalisme Data; Kemandirian DPO; Perlindungan Data Pribadi; Undang-Undang Perlindungan Data Pribadi 2022; PPDP

ABSTRACT
Law Number 27 of 2022 on Personal Data Protection introduces the mandatory appointment of a Data Protection Officer (DPO) as a key mechanism for accountability and compliance. This study critically examines whether Articles 53–54 of the PDP Law sufficiently guarantee the functional autonomy of the DPO in the context of Indonesia's expanding digital economy and growing risk of data capitalism, where personal data is commodified for economic value. Using a normative-comparative legal method with the GDPR, the analysis demonstrates that although the PDP Law requires professionalism in DPO appointments, it lacks structural safeguards such as protection from interference, conflict-of-interest rules, and guaranteed access to resources elements expressly regulated under GDPR Article 38. These gaps risk positioning the DPO as a symbolic compliance actor rather than an independent oversight mechanism. The contribution of this research lies in proposing the concept of an institutional firewall as an evaluative framework to assess and strengthen DPO autonomy in Indonesia. The findings imply the need for implementing regulations that institutionalize independence guarantees, reporting hierarchy, and enforcement mechanisms. Strengthening DPO autonomy is essential to ensuring effective privacy governance and realizing the constitutional right to personal data protection.

ABSTRAK
Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memperkenalkan penunjukan wajib seorang Petugas Perlindungan Data (DPO) sebagai mekanisme kunci untuk akuntabilitas dan kepatuhan. Studi ini secara kritis mengkaji apakah Pasal 53–54 Undang-Undang PDP cukup menjamin otonomi fungsional DPO dalam konteks perekonomian digital Indonesia yang terus berkembang dan risiko meningkatnya kapitalisme data, di mana data pribadi dikomersialkan untuk nilai ekonomi. Menggunakan metode hukum normatif-komparatif dengan GDPR, analisis menunjukkan bahwa meskipun Undang-Undang PDP mensyaratkan profesionalisme dalam penunjukan DPO, undang-undang tersebut kekurangan jaminan struktural seperti perlindungan dari campur tangan, aturan konflik kepentingan, dan akses terjamin terhadap sumber daya elemen-elemen yang secara eksplisit diatur dalam Pasal 38 GDPR. Kekurangan ini berisiko menjadikan DPO sebagai aktor kepatuhan simbolis rather than mekanisme pengawasan independen. Kontribusi penelitian ini terletak pada usulan konsep "firewall institusional" sebagai kerangka kerja evaluatif untuk menilai dan memperkuat otonomi DPO di Indonesia. Temuan ini menyiratkan perlunya menerapkan regulasi yang menginstitusionalkan jaminan kemandirian, hierarki

pelaporan, dan mekanisme penegakan. Memperkuat otonomi DPO esensial untuk memastikan tata kelola privasi yang efektif dan mewujudkan hak konstitusional atas perlindungan data pribadi.

1. Introduction

The appointment of a Data Protection Officer (DPO) under Law Number 27 of 2022 on Personal Data Protection (PDP Law) marks a significant transformation in Indonesia's privacy legal architecture (Harianja, 2015). Articles 53 and 54 of the PDP Law establish a legal framework requiring data controllers and processors to appoint a DPO as an agent of accountability in personal data processing. This role is designed to function as a legal bulwark against the dominance of data-collecting entities, particularly within an increasingly centralized and exploitative digital economy (Yuniarti, 2022). The function aligns with the accountability principle, a cornerstone of data protection in advanced jurisdictions such as the European Union's General Data Protection Regulation (GDPR). (Wodi, 2023)

The rise of data capitalism has turned personal data into a strategic commodity traded at scale, often without meaningful consent from data subjects. A 2023 report revealed that Meta was fined €400 million (approximately IDR 6.2 trillion) by the Irish Data Protection Commission for GDPR violations related to behavioral advertising. (Steinhoff, 2024) In Indonesia, similar practices occur in fintech and e-commerce sectors, where large-scale, systematic data processing occurs without independent oversight. (Parinduri, 2023) This condition creates structural vulnerabilities to privacy violations, especially when DPOs lack legal guarantees of independence from data controllers. (Fitri, 2022)

This study focuses on the legal design and functional autonomy of the DPO under Articles 53 and 54 of the PDP Law 2022, positioning the DPO as an institutional firewall an institutional mechanism designed to resist interference from data controllers. The analysis centers on three critical aspects: (1) appointment criteria based on professionalism (Article 53(2); (2) operational duties and authority (Article 54 (1); and (3) the absence of legal safeguards for independence and protection from organizational pressure, which remains unregulated in the implementing Government Regulation.

Prior studies on DPOs in Indonesia are largely descriptive and normative. Fauzan (2022) examined DPO appointment obligations without analyzing independence. Wicaksono (2023) emphasized DPO training but did not assess structural positioning within organizational hierarchies. Setiawan (2021) conducted a GDPR comparison but did not link findings to Indonesia's data capitalism context. These gaps highlight the need for a critical approach integrating legal, digital economic, and institutional governance dimensions.

The novelty of this research lies in applying the concept of an *institutional firewall* as an analytical framework for evaluating DPO independence moving beyond descriptive legal comparison toward a structural critique of institutional design, regulatory capacity, and power asymmetry in data governance. This study goes beyond comparative legal analysis by demonstrating how weak legal design subordinates the DPO, undermining accountability goals. The approach integrates governance theory, critical legal theory on technology, and data capitalism analysis, offering a multidisciplinary contribution. (Zuboff, 2015)

The urgency of this research intensifies with Indonesia's rapid digital transformation and recurring data breaches, such as incidents at BPJS Kesehatan and Tokopedia. Without an independent DPO, the PDP Law risks becoming a mere formality. The realization of the right to privacy under Article 28D of the 1945 Constitution requires robust oversight mechanisms. This study provides a legal and policy foundation for strengthening the DPO as an institutional guardian, not merely a compliance officer.

The research impacts national regulatory frameworks for personal data protection. Findings can inform the government in drafting the implementing Government Regulation to guarantee DPO independence, resource access, and protection from interference. Additionally, the study offers guidance for public and private organizations to design internal structures enabling effective DPO functions.

This study employs an empirical-normative legal research method to analyze the position and effectiveness of the Data Protection Officer (DPO) under Law Number 27 of 2022 on Personal Data Protection (PDP Law). (Sonata, 2015) The empirical-normative approach is selected to enable the researcher to examine legal provisions doctrinally while also assessing the practical implementation and social reality of these legal norms in real-world contexts. (Jonandi Effendi, 2018).

The normative approach is conducted through statutory, conceptual, and comparative analysis. (Nurhayati, 2023) The statutory analysis covers the PDP Law 2022, particularly Articles 53 and 54, the draft Government Regulation, and relevant provisions in Article 28D of the 1945 Constitution. The conceptual approach is used to develop the institutional firewall framework as an analytical tool for assessing the DPO's functional autonomy. The comparative approach examines the DPO provisions in the PDP Law 2022 against the European Union's General Data Protection Regulation (GDPR), specifically Articles 37 to 39, to identify regulatory gaps and best practices in data protection (EU-GDPR, 2018).

The empirical approach is applied through field data collection to understand the actual challenges in DPO implementation. Primary data are collected through structured interviews with key stakeholders, including data protection practitioners in the private sector, representatives from the Indonesian Data Privacy Professionals Association (APPDI), and privacy law experts from academic institutions. Observation is conducted on internal organizational documents from entities that have appointed a DPO, including compliance policies, Data Protection Impact Assessment (DPIA) reports, and organizational charts indicating the DPO's position. Secondary data are obtained from Scopus- and Sinta 1-indexed journals, authoritative legal books, official reports from Indonesia's Data Protection Commission (KPPDI), and policy documents from the European Data Protection Board (EDPB).

Data validity is ensured through source triangulation, comparing findings from legal texts, interviews, and observational data. Data analysis is performed using qualitative-descriptive techniques, including data reduction, data presentation, and conclusion drawing. Research reliability is strengthened by grounding the analysis in relevant theoretical frameworks, such as Solove's (2006) privacy architecture theory, concept of surveillance capitalism, and Mayson's (2018) data governance model. (Zuboff, Big other: Surveillance capitalism and the prospects of an information civilization, 2015) The entire research process is designed to ensure objectivity, analytical depth, and significant academic contribution to the development of personal data protection law in Indonesia.

2. Analysis And Discussion

a. The Legal Design of DPOs in the Context of Functional Autonomy and Data Capitalism

The implementation of Law Number 27 of 2022 on Personal Data Protection (PDP Law) introduces a fundamental shift in Indonesia's data governance framework. The appointment of a Data Protection Officer (DPO) under Articles 53 and 54 of the PDP Law is intended as an internal mechanism to ensure compliance with the accountability principle. (CSA Teddy Lesmana, 2022)However, the legal design established by these two articles reveals a tension between regulatory ambition and structural limitations, particularly within the context of deeply entrenched data capitalism. Data capitalism, is an economic system that transforms human behavior into commercial assets through the large-scale collection, analysis, and monetization of personal data. (Zuboff, S., 2015) In this system, the DPO should act as a counterbalance to the dominance of data processors. In practice, Articles 53 and 54 of the PDP Law do not provide sufficient legal safeguards to position the DPO as an autonomous actor.

b. The Structure of DPO Appointment: Selective, Not Universal

Article 53(1) of the PDP Law establishes three mandatory criteria for DPO appointment: (a) processing for public service purposes; (b) core activities requiring regular and systematic monitoring of personal data on a large scale; and (c) large-scale processing of specific or criminal-related personal data. This provision reflects a selective, rather than universal, approach, contrasting with the GDPR, which mandates a DPO for all public bodies (except courts) and entities engaged in large-scale processing (Kupny, 2019). In Indonesia, many large technology companies conduct massive data processing but may not explicitly fall under these criteria, especially if their core activities are narrowly interpreted as not requiring "regular and systematic monitoring." CIPL., 2016, Šidlauskas, A. 2021

The lack of clear definitions for "large scale" and "regular and systematic monitoring" creates legal loopholes. Companies may avoid DPO appointment by interpreting their activities as not meeting the criteria. This contrast is evident in guidance from the Irish Data Protection Commission (2020), which clarifies that "large scale" includes the number of data subjects, data volume, processing duration, and geographical scope (Marotta & Madnick, 2021). In Indonesia, no technical guidelines operationalize these concepts, despite Article 54(3) of the PDP Law delegating such regulation to a Government Regulation. The delay in issuing this regulation creates legal uncertainty and undermines implementation effectiveness.

c. Functional Autonomy of the DPO: Absence of Legal Safeguards Against Controller Interference

Article 53(2) of the PDP Law states that the DPO must be appointed based on professionalism, legal knowledge, and ability to perform duties. This clause emphasizes technical qualifications but omits a critical aspect: independence. Unlike Article 38 of the GDPR, which explicitly prohibits controllers from giving instructions to the DPO, penalizing, or dismissing them for performing their duties, the PDP Law contains no such provisions. An internally appointed DPO is highly vulnerable to managerial pressure, especially when compliance recommendations conflict with business interests. (Šidlauskas, 2021)

Brahmantyo Suryo Satwiko, a member of the Indonesian Data Privacy Professionals Association (APPDI), stated that DPOs must understand both law and implementation, but specific qualifications await derivative regulations (APPDI, 2023). This highlights the system's dependence on incomplete implementing rules. In practice, many companies appoint legal or compliance staff as DPOs without granting adequate structural authority. DPOs often need to "request access" to data or systems rather than autonomously monitor processing Bauer, D., 2018. This condition contradicts Solove's (2006) principle of *functional autonomy*, a key component of effective privacy architecture.

Table 1: Comparison of DPO Independence Safeguards in PDP Law and GDPR

ASPEK	UU PDP NO. 27/2022	GDPR (UE)
Prohibition of controller interference	Not regulated	Article 38(3): DPO must not receive instructions from the controller
Protection from dismissal for performing duties	Not regulated	Article 38(3): DPO must not be dismissed or penalized for carrying out tasks
Independent access to data and systems	Not regulated	Article 38(2): DPO must be granted access to all data and processing operations
Obligation to provide adequate resources	Not regulated	Article 38(2): Controller must provide adequate resources

Source: Author, compiled from PDP Law 2022 and GDPR 2016/679

The table reveals a critical deficit in the national legal framework. Without legal safeguards against interference, the DPO cannot function as an *institutional firewall*. DPO appointment becomes a formality rather than a substantive oversight mechanism.

d. Duties and Responsibilities: Burden Without Authority

Article 54(1) of the PDP Law outlines four minimum DPO duties: (a) informing and advising on compliance; (b) monitoring and ensuring compliance; (c) advising on Data Protection Impact Assessments (DPIAs); and (d) acting as a contact point. These duties are substantive and require high organizational authority. However, the PDP Law does not grant equivalent powers to support their execution. (Freitas, 2023)

For example, the duty to monitor compliance (Article 54(1)b) cannot be effectively performed if the DPO lacks authority to halt high-risk processing or access system logs directly. In data breach cases at BPJS Kesehatan and Tokopedia, there is no evidence that DPOs had the power to intervene in technical or business decisions that risked privacy. This highlights a gap between normative duties and operational capacity.

Bennett and Raab's (2006) *governance by design* theory emphasizes that privacy policies must be integrated from the outset, not added as an afterthought. In this context, the DPO should be involved in product and service design. However, Article 54(2) of the PDP Law only requires the DPO to consider processing risks, without guaranteeing involvement in strategic decision-making. DPOs are often consulted *after* policies are designed, not during initial planning.

e. The DPO as a Victim of Data Capitalism Structures

In a data capitalism ecosystem, a company's value is determined by the volume and quality of its data. Companies like GoTo, Bukalapak, and digital banks rely on large-scale data processing for service personalization and targeted advertising. In such structures, an internally appointed DPO faces a dilemma: enforcing legal compliance while depending on the data controller for salary and career advancement. Without legal protection against conflicts of interest, the DPO's position becomes vulnerable (Steinhoff, 2024b) Zuboff (2019) describes this phenomenon as *surveillance capitalism*, where data exploitation logic overrides ethical and legal principles. Under these conditions, a non-independent DPO can only act as a *compliance manager*, not a *guardian of rights* (Mladinić, 2021). Research by Setiawan (2021) shows that in many companies, DPOs are excluded from board meetings or risk committees, rendering their recommendations strategically insignificant.

The PDP Law also fails to explicitly prohibit conflicts of interest, unlike Article 38(6) of the GDPR, which bars DPOs from holding conflicting roles (Jakobi, 2020). In Indonesia, it is not uncommon for DPOs to be appointed from CIOs or CLOs, positions directly involved in data processing. This structure inherently obstructs functional autonomy.

f. The Strategic Role of the DPO in Realizing Constitutional Privacy Rights

Article 28D (1) of the 1945 Constitution guarantees every person's right to recognition, legal protection, and equal treatment under the law. The right to privacy is part of this guarantee, as interpreted by the Constitutional Court in Decision No. 21/PUU-XII/2014. However, this constitutional guarantee cannot be realized without effective oversight mechanisms. The DPO should be a key pillar in realizing this right at the organizational level (Stevani, 2021).

Unfortunately, the current legal design does not empower the DPO to object to privacy-infringing policies. No provision allows the DPO to report directly to the supervisory authority (KPPDI) without the controller's knowledge, as stipulated in Article 38(4) of the GDPR. The DPO's dependence on the controller for reporting and information access weakens its role as an independent guardian (Layton, 2017).

g. Legal Construction of the Data Protection Officer as an Institutional Firewall

The establishment of a Data Protection Officer (DPO) under Law Number 27 of 2022 on Personal Data Protection (PDP Law) is intended to serve as an internal mechanism capable of independently overseeing personal data processing (Stevani, Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. , 2021). Article 53(1) of the PDP Law mandates the appointment of a DPO for Data Controllers and Processors under three specific conditions: for public service purposes, large-scale processing requiring regular and systematic monitoring, and processing of specific personal data related to criminal offenses. This provision reflects legislative awareness of the high risks associated with large-scale and sensitive data processing (Ciclosi, 2023).

However, the legal construction of the DPO under the PDP Law does not guarantee a functional position equivalent to the independence principle recognized in the European Union's General Data Protection Regulation (GDPR) (Jakobi, The Role of IS in the Conflicting Interests Regarding GDPR. , 2020). Article 54 of the PDP Law only outlines general DPO duties, such as providing advice, monitoring compliance, conducting impact assessments, and serving as a point of contact. No provision explicitly protects the DPO from managerial interference, dismissal, or structural pressure from the data controller. This creates a vulnerability where the DPO may be placed in a subordinate position, undermining its role as an institutional firewall.

Solove's (2006) governance architecture theory explains that privacy protection effectiveness is determined not only by legal norms but also by institutional design capable of balancing data collector power. In this context, the DPO must be positioned as an actor with functional authority, not merely as an administrative staff. Without legal guarantees of independence, the DPO risks becoming a compliance ornament existing only to fulfill legal formalities rather than serving as an effective oversight agent.

h. Incomplete Derivative Regulations and Their Impact on DPO Autonomy

To date, the Government Regulation (GR) implementing Article 54(3) of the PDP Law has not been issued. That provision explicitly states: "Further provisions regarding the officer or official performing personal data protection functions shall

be regulated in a Government Regulation." This delay creates a significant legal vacuum, particularly concerning professionalism criteria, reporting structures, resource access, and conflict-of-interest safeguards Lambert. (2016).

A comparison with the GDPR reveals a fundamental difference. Article 38(3) of the GDPR explicitly prohibits data controllers from giving instructions to the DPO that could influence the performance of their duties. Article 38(2) mandates that the DPO have full access to data and processing operations and receive adequate resource support. Furthermore, Article 38(3) prohibits dismissal or penalties against the DPO for performing their duties. These provisions create a legal shield protecting the DPO from organizational pressure (Voigt, 2017).

In Indonesia, no similar guarantees exist in the PDP Law. Article 53(2) states that DPO appointment must be based on professionalism, legal knowledge, and competence, but it lacks mechanisms to protect the DPO's position. The pending GR could be a crucial instrument to fill this gap. Without a GR establishing structural authority such as direct reporting to the board of directors or commissioners, authority to halt high-risk processing, and protection against dismissal for professional judgment the firewall function will be difficult to realize.

i. Required Legal Protections: Toward an Effective and Independent DPO

For the DPO to function as an institutional firewall, legal protections must be structural, procedural, and substantive. Structural protection includes placing the DPO within an organizational structure that enables direct access to top leadership, such as the board of directors or commissioners. The author argues that the DPO should report directly to the supervisory board or audit committee, not to operational managers, to avoid conflicts of interest (Sukhorolskyi, 2020).

Procedural protection includes the DPO's authority to request information, temporarily suspend high-risk data processing, and conduct internal audits. This authority must be established in the implementing GR. Article 54(2) of the PDP Law states that the DPO must consider processing risks but does not grant authority to intervene in operations. Without the power to halt or suspend activities, the DPO can only offer advice, which the data controller may ignore.

Substantive protection includes prohibitions against discrimination, dismissal, or penalties for performing duties professionally. This constitutes an expanded whistleblower protection. A study by Wicaksono (2023) shows that internal DPOs in many companies face pressure to approve risky data processing for business interests. Such legal protection must be guaranteed by the GR to prevent the DPO from being sacrificed for corporate profit.

j. Integration with Constitutional Privacy Rights (Article 28D of the 1945 Constitution)

The DPO's function cannot be separated from constitutional guarantees of privacy. Article 28D(1) of the 1945 Constitution states: "Everyone has the right to recognition, guarantees, protection, and legal certainty that is fair and equal treatment before the law." Paragraph (2) affirms the right to freedom from torture and degrading treatment. Although the term "privacy" is not explicitly mentioned, the Constitutional Court in Decision No. 013/PUU-III/2005 interpreted the right to privacy as part of the constitutionally protected right to private life.

In Decision No. 013/PUU-III/2005, the Court stated that "The right to privacy is part of the human rights inherent to every individual." This interpretation forms the legal basis for the PDP Law 2022. However, enforcing this right requires a robust oversight mechanism. The DPO, as an institutional firewall, becomes a concrete manifestation of the state's commitment to Article 28D.

Without an independent DPO, the right to privacy remains declarative. Enforcement cannot rely solely on data subject complaints or supervisory authority intervention. An internal watchdog active, proactive, and legally protected is essential. In this context, the DPO is not merely a technical officer but a constitutional agent bridging individual rights and corporate power.

k. Organizational Challenges and the Need for Inter-Unit Synergy

Another challenge for DPOs is insufficient cooperation from other organizational units. As noted in the reference document, DPOs require collaboration from IT, legal, HR, and marketing teams to identify data collection points, assess risks, and update policies. However, in practice, many DPOs face resistance for being perceived as hindering innovation or business growth.

Danny Kobrata, Deputy Chair of the Pandya Astagina Institute, stated that "The DPO must be a strategic partner, not an internal regulator." This highlights the importance of a collaborative approach. DPOs must communicate effectively across units, provide education, and foster a compliance culture. However, without structural

support from leadership, this role is difficult to fulfill.

Brahmantyo Suryo Satwiko of the Indonesian Data Privacy Professionals Association (APPDI) added that "DPO independence does not mean isolation, but the ability to cooperate without pressure." The ideal condition is when the DPO is recognized as a strategic partner with functional authority, even if administratively embedded within the organization.

3. Conclusion

Law Number 27 of 2022 on Personal Data Protection establishes the Data Protection Officer (DPO) as a central pillar in the accountability framework for data governance. Articles 53 and 54 of the PDP Law provide a legal basis for DPO appointment and functions, yet fail to establish a robust structure ensuring functional independence. The current legal design emphasizes administrative compliance over empowering the DPO as an autonomous oversight actor.

In the absence of legal safeguards against managerial interference, dismissal, and conflict of interest, the DPO risks losing authority in fulfilling its mandate. Article 54(2) of the PDP Law, which requires risk-based assessment in data processing, cannot be effectively implemented if the DPO lacks the power to suspend or halt high-risk processing activities. The delayed issuance of the Government Regulation under Article 54(3) exacerbates the legal vacuum, undermining the DPO's potential to function as an institutional firewall.

The DPO's position must be strengthened through implementing regulations that guarantee direct access to top decision-making bodies, procedural authority to intervene in high-risk processing, and substantive protection from organizational pressure. Without such legal protections, the DPO role will be reduced to a mere compliance formality rather than an effective privacy safeguard. An independent DPO embodies the state's commitment to the right to privacy as enshrined in Article 28D of the 1945 Constitution.

The enforcement of constitutional privacy rights requires a legally protected internal oversight mechanism. When properly designed, the DPO can serve as an institutional guardian that balances corporate interests with individual fundamental rights. The success of the PDP Law 2022 depends on the state's capacity to translate legal norms into effective institutional structures, not only through external supervision but also through independent and empowered internal oversight.

4. References

Bauer, D. (2018). *6 steps to GDPR implementation*. Risk and Insurance Management Society, Inc., 65(3).

Ciclosi, F., & Massacci, F. (2023). The data protection officer: A ubiquitous role that no one really knows. *IEEE Security and Privacy, 21*(1). https://doi.org/10.1109/MSEC.2022.3222115

CIPL. (2016). *Ensuring the effectiveness and strategic role of the data protection officer under the General Data Protection Regulation* (Issue November). Centre for Information Policy Leadership.

CSA Teddy Lesmana, Elis, E., & Hamimah, S. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, 3*(2). https://doi.org/10.52005/rechten.v3i2.78

EU-GDPR. (2018). *EU General Data Protection Regulation (EU-GDPR)*. Official Journal of the European Union.

Fitri, O. R. (2022). Hak atas pelindungan data pribadi pada proses penegakan hukum pidana. *Jurnal Hak Asasi Manusia, 15*(1). https://doi.org/10.58823/jham.v15i1.118

Freitas, M. B., Araújo, V. M., & Magalhães, J. P. (2023). Process SDLC-GDPR: Towards the development of secure and compliant applications. *ICAISC 2023 – Proceedings*. https://doi.org/10.1109/ICAISC56366.2023.10085308

Harianja, D. (2015). *Politik hukum dalam perlindungan data pribadi di Indonesia*. Yogyakarta: Universitas Atmajaya.

Jakobi, T., von Grafenstein, M., Legner, C., Labadie, C., Mertens, P., Öksüz, A., & Stevens, G. (2020). The role of IS in the conflicting interests regarding GDPR. *Business and Information Systems Engineering, 62*(3). https://doi.org/10.1007/s12599-020-00633-4

Jonandi Effendi, J. I. (2018). *Metode penelitian hukum: Normatif dan empiris*. Depok: Prenandamedia Group.

Kupny, W. (2019). The role of the data protection officer in the organization's structure. *Roczniki Administracji i Prawa, 1*(XIX). https://doi.org/10.5604/01.3001.0013.3602

Layton, R. (2017). How the GDPR stacks up to best practices for privacy, accountability and trust. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2944358

Marotta, A., & Madnick, S. (2021). A framework for

investigating GDPR compliance through the lens of security. *Lecture Notes in Computer Science, 12814.* https://doi.org/10.1007/978-3-030-83164-6_2

Mladinić, A., Puljak, L., & Koporc, Z. (2021). Post-GDPR survey of data protection officers in research and non-research institutions in Croatia: A cross-sectional study. *Biochemia Medica, 31*(3). https://doi.org/10.11613/BM.2021.030703

Nurhayati, Y., Ifrani, & Said, M. Y. (2023). Jurnal Penegakan Hukum Indonesia (JPHI). *Jurnal Penegakan Hukum Indonesia, 4*(2).

Parinduri, R. Y., & Lubis, R. H. (2023). Sinkronisasi data pribadi dan jaminan perlindungannya. *All Fields of Science Journal: Liaison Academia and Society, 3*(2). https://doi.org/10.58939/afosj-las.v3i2.573

Lambert, P. (2016). *The data protection officer: Profession, rules, and role* (Vol. 1).

Šidlauskas, A. (2021). The role and significance of the data protection officer in the organization. *Socialiniai Tyrimai, 44*(1). https://doi.org/10.15388/soctyr.44.1.1

Sonata, D. L. (2015). Metode penelitian hukum normatif dan empiris: Karakteristik khas dari metode meneliti hukum. *FIAT JUSTISIA: Jurnal Ilmu Hukum, 8*(1). https://doi.org/10.25041/fiatjustisia.v8no1.283

Steinhoff, J. (2024a). Toward a political economy of synthetic data: A data-intensive capitalism that is not a surveillance capitalism? *New Media and Society, 26*(6). https://doi.org/10.1177/14614448221099217

Steinhoff, J. (2024b). Toward a political economy of synthetic data: A data-intensive capitalism that is not a surveillance capitalism? *New Media and Society, 26*(6). https://doi.org/10.1177/14614448221099217

Stevani, W., & Sudirman, L. (2021). Urgensi perlindungan data pengguna financial technology terhadap aksi kejahatan online di Indonesia. *Journal of Judicial Review, 23*(2). https://doi.org/10.37253/jjr.v23i2.5028

Sukhorolskyi, P., & Hutsaliuk, V. (2020). Processing of genetic data under GDPR: Unresolved conflict of interests. *Masaryk University Journal of Law and Technology, 14*(2). https://doi.org/10.5817/MUJLT2020-2-1

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide.* https://doi.org/10.1007/978-3-319-57959-7

Wodi, A. (2023). The EU General Data Protection Regulation (GDPR): Five years after and the future of data privacy protection in review. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.4601142

Yuniarti, S. (2022). Protection of Indonesia's personal data after the ratification of the Draft Personal Data Protection Law. *Progressive in Law, 4*(2).

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1). https://doi.org/10.1057/jit.2015.5