SHIOSHYA
Studies and Perspectives on Law and Justice

Vol. 2
No. 1
January 2026
pp. 47–63

Organizational Communication Ethics and Personal Data Protection: A Review of the Personal Data Protection Law

Wanda Iqwatul Qofifah [a,1*], Muhammad Dirgantara [b,2], Fadhlan Maulana [c,3], Zul Fahmi [d,4]

[a] Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda, Jl. H. A. M. Rifaddin, Samarinda, Kalimantan Timur 75251, Indonesia
[b] Institut Agama Islam Negeri Parepare, Jl. Amal Bhakti No. 8, Soreang, Parepare, Sulawesi Selatan 91131, Indonesia
[c] Institut Agama Islam Negeri Fattahul Muluk Papua, Jl. Merah Putih Buper Waena, Distrik Heram, Jayapura, Papua 99142, Indonesia
[d] Sekolah Tinggi Agama Islam Negeri Mandailing Natal, Jl. Prof. Dr. Andi Hakim Nst, Mandailing Natal, Sumatra Utara 22977, Indonesia

[1] wandaqofifah@gmail.com*, [2] muhammaddirgantara86@gmail.com, [3] fadhlanmaulana040@gmail.com, [4] zulfahmi1901@gmail.com
* Corresponding Author

ARTICLE INFORMATION

Article History
Accepted : December 27, 2025
Revised : January 6, 2026
Accepted : January 8, 2026

Keywords
Communication Ethics
Informed Consent
Organizational Communication
Personal Data Protection
Public Relations

ABSTRACT

This study examines the relationship between organizational communication ethics and the legal framework for Personal Data Protection in Indonesia, with a focus on Law No. 27 of 2022 (PDP Law). Using a qualitative approach based on library research and normative analysis of regulatory texts and academic literature, this study combines contextual integrity theoretical framework and privacy damage map to evaluate the compatibility between ethical principles (informed consent, transparency, accountability, minimization) and the legal provisions contained in Articles 20–21, Articles 30–46, Articles 51–56 of the PDP Law. The findings show that the PDP Law provides a normative foundation that is in line with ethical principles of communication, such as recognition of subject rights, DPIA obligations, and data breach notification obligations, but there is an operational gap due to formalistic consent practices, dependence on third parties, limited institutional capacity, and unfinished implementing regulations. This study also compares international experiences from 13 countries, such as the EU GDPR, Singapore's PDPA, China's PIPL, and other country models to formulate adaptive lessons. Recommendations include the implementation of privacy by design, a pre-campaign DPIA checklist, standardization of concise privacy notices and granular consent options, strengthening the role of the DPO and strict contractual clauses with vendors, and accelerating implementing regulations and capacity building programs. The novelty of the research lies in the integrative mapping of articles versus ethical principles, which produces specific operational recommendations for public relations units and policymakers.

1. Introduction

The development of digital technology over the past decade has accelerated the flow of information and changed the way organizations collect, process, and store personal data (Imran et al., 2021; Paul et al., 2024). The scale of data breaches and incidents shows a significant upward trend, with many international empirical studies noting a surge in the average cost of handling breaches and the number of accounts exposed, signaling major financial and reputational risks for organizations (Avanzi et al., 2025; Li et al., 2023; Zhang et al., 2022). Globally, the average cost of data breaches continues to rise and the volume of exposed accounts has skyrocketed in recent years (see Figure 1) (White & Koskey, 2025).

In the Indonesian context, a number of major incidents involving data leaks from platforms and government agencies confirm that this vulnerability is real and recurring. According to a report by

Surfshark, Indonesia ranks 13th globally in terms of the number of data leaks, with a total of 156.8 million data leaks since 2004 to April 15, 2024 (Latifa, 2024). Some of these incidents involve the leakage of personal data from important state institutions (see Table 1) (Toruan, 2025). These facts make personal data protection a strategic issue for modern organizational communication practices.

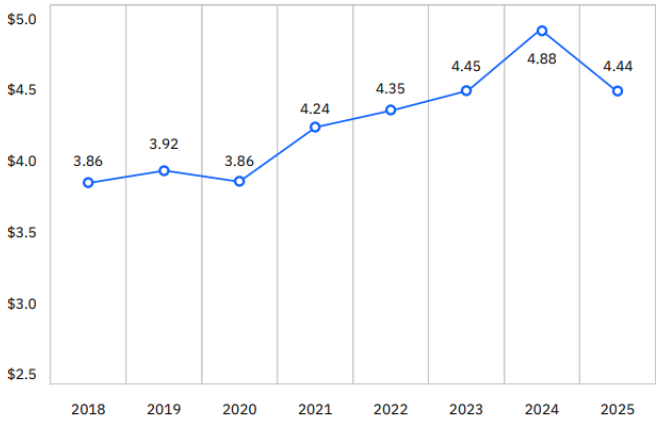

Figure 1. Global Data Breach Costs (measured in millions of USD), Source: White & Koskey (2025).

Table 1. Personal Data Breaches in Indonesia (2023-2024)

Agency/Institution	Year	Data Breach
Directorate General of Population and Civil Registration (Dukcapil)	2023	Approximately 337 million resident data
Bank Syariah Indonesia (BSI)	2023	Approximately 15 million customer data
Official YouTube channel of the House of Representatives (DPR)	2023	Approximately 2 million customer data
Taxpayer Identification Number (NPWP)	2024	Approximately 6 million data
Temporary National Data Center (PDNS) 2 Surabaya	2024	Approximately USD 8 in damages

Source: Toruan (2025).

The urgency of organizational communication ethics arises from the need to balance corporate communication objectives with respect for individual privacy rights, such as transparency, marketing, and public relations (Fritz, 2022; Shaya & Ahmad, 2024). Public relations and public communication practices often involve the collection and publication of data on customers, stakeholders, and audiences, which, if not managed ethically, can lead to rights violations, loss of trust, and legal sanctions (Çelik et al., 2025; Görpe & Öksüz, 2024; Sutherland et al., 2020).

In Indonesia, this context is further reinforced by the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which regulates the rights of data subjects and the obligations of controllers (Republik Indonesia, 2022), but ethical challenges remain complex due to formalistic consent practices, the use of third parties, and the need for organizations to remain effective in communication (Supeno et al., 2025; Widiatedja & Mishra, 2023). Therefore, a study of the ethics of organizational communication within the legal framework is urgent.

Several relevant previous studies have provided for this study. Studies on ethical challenges in digital public relations by Hagelstein et al. (2024) and Ashby-King et al. (2025) show that ethical values such as authenticity of consent and data protection need to be internalized in public relations practices so that they do not become mere administrative formalities. Their research emphasizes the need for procedures that are capable of responding to the realities of digital practices. Recent research by Yourell et al. (2025) in digital health companies shows a positive relationship between privacy policy compliance, technological ethical awareness, and user privacy protection, indicating that regulation needs to be balanced by the capacity of organizations to implement technical ethics and governance. These findings are relevant for framing normative hypotheses in library research studies.

Other relevant studies highlight aspects of law enforcement and data breach cases in Indonesia. One study by Abdillah et al. (2024) on the frequency and factors causing national data breaches shows a pattern of recurring technical and procedural weaknesses, confirming that the risks are not only technical but also organizational. In addition, studies examining the obstacles to the implementation of the PDP Law in Indonesia and comparing it with other countries, such as studies by Syailendra et al. (2024), Natamiharja & Setiawan (2024), and 'Aisyi et al. (2025), identify real obstacles, such as the unfinished derivative regulations and the absence of a strong supervisory authority, which can have implications for the effectiveness of legal protection. The aforementioned studies have provided a critical context for ethical studies because they reveal the gap between expected legal norms and data management practices in the field.

Based on a review of the literature and regulatory developments, there is a clear research gap, although there are technical studies and studies on the implementation of the law, there are still few studies that specifically combine an analysis of organizational communication ethics with a normative review of the provisions of the PDP Law. The novelty of this research lies in its integrative approach—linking ethical principles of communication, such as informed consent, transparency, data minimization, and non-maleficence, with an analysis of the provisions in the PDP Law to assess the extent to which legal provisions provide an ethical basis for public relations practices, as well as to identify areas where professional ethics must fill regulatory gaps. In addition, this study offers practical recommendations based on a legal vs. ethical matrix that can be directly applied by organizational communication units.

The research question in this study is how the provisions of the PDP Law regulate the responsibility of organizational communication towards data subjects, as well as which principles of organizational communication ethics are most crucial and problematic when faced with the provisions of the PDP Law in public relations practice. The objectives of this study are to analyze key articles in the PDP Law that are relevant to organizational communication practices, evaluate the compatibility and contradictions between legal provisions and ethical communication principles, and develop ethical recommendations and practical policies for public relations units to enable them to fulfill their legal obligations while maintaining the integrity of communication ethics.

2. Literature Review

2.1. Contextual Integrity

The theory proposed by Nissenbaum (2004) places privacy not as an abstract right or mere individual control over data, but rather as compliance with norms of information sharing determined by a specific social context. According to this theory, the appropriateness of data exchange is assessed using three main parameters: (1) actors, namely who sends and receives the data; (2) attributes, namely the type or nature of the information; and (3) transmission principles, namely the principles or conditions that govern the flow of information, such as consent, confidentiality, or purpose of use.

When one of these parameters changes, contextual integrity is violated. For example, data that was originally shared in the context of healthcare services is suddenly published for commercial purposes (de Groot, 2024). This theory of contextual integrity is useful for analyzing organizational communication because it requires a normative evaluation of digital data collection and dissemination practices in accordance with different communication contexts, rather than merely technical compliance with regulations (Kumar et al., 2024).

2.2. Taxonomy of Privacy

Solove (2006) offers a taxonomy of privacy that helps identify how privacy violations impact individuals and society. Instead of defining privacy as a single concept, this theory groups violations into several categories, namely collection, storage, processing, and dissemination. Collection refers to excessive data collection; the storage category can include the risks of accumulation and profiling; processing includes misuse or misleading analysis; and dissemination can take the form of leaks or unauthorized publication (de Oliveira-Martins & Gonçalves-Sant'Ana, 2024; Rabitti et al., 2025).

In addition, there is the category of invasion, which includes surveillance and personal intrusion. This taxonomy of privacy map facilitates ethical assessment because every organizational communication action can be inventoried according to the type of potential damage, such as whether it increases the risk of discrimination, damages reputation, reduces individual autonomy, or causes fear or discomfort (Chapman et al., 2025). This framework is useful for formulating mitigation concepts that are both ethical and operational.

2.3. Organizational Communication Ethics

In the realm of organizational communication ethics, there are several core principles that complement each other: informed consent, accountability, transparency, and non-maleficence (Bisel & Mahutga, 2024). Informed consent requires that the subject's consent be based on sufficient, clear, and accessible information that is not merely a legalistic checkbox. This requires a communication format that is easily understood by the audience (van Goidsenhoven & de Schauwer, 2022). Accountability means that organizations are responsible for data management policies and practices—including documentation, internal audits, and remediation mechanisms in the event of violations (Mager et al., 2025; Wasserman, 2024).

Then there is transparency, which requires organizations to explain the purpose, scope, and parties that have access to the data, so that the public can assess the risks and benefits (Lee & Li, 2021). Non-maleficence, or the principle of doing no harm, requires organizations to minimize potential harm through data minimization, technical protection, and ethical use policies (Croce, 2023). Together these principles provide a normative foundation that can be operationalized in public relations policies and organizational communication guidelines related to personal data.

3. Methods

This research method is qualitative in nature, using a library research approach and normative-analytical analysis of documents (Rushagama, 2024). Primary data analyzed includes the text of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and relevant regulations. Secondary data consists of academic literature in the form of journal articles, books, institutional reports, verified media articles, and published privacy policies or internal organizational standards. Analysis stage uses close reading and thematic content analysis techniques to extract legal norms, controller obligations, and ethical issues that arise in organizational communication practices.

The findings are reduced to a norm vs. ethical principle analysis matrix that facilitates direct comparison between legal provisions and professional ethical demands. Analytical process includes document codification, grouping of ethical themes, and synthesis of normative arguments to formulate practice and policy recommendations. Validity of the findings is maintained through source triangulation, transparent documentation of the analysis steps, and cross-checking of primary references (Christou, 2022; Santos et al., 2020).

4. Results and Discussion

4.1. Organizational Communication under the PDP Law

The PDP Law contains a series of data subject rights that directly impact organizational communication practices, particularly the rights of access, correction, transfer, and deletion of data (Supeno et al., 2025; Syailendra et al., 2024; Widiatedja & Mishra, 2023). The technical provisions regarding access rights and the obligation to correct or provide copies are contained in Articles 30 to 33, which read as follows (Republik Indonesia, 2022):

> Article 30 paragraph (1): "The Personal Data Controller shall update and/or correct errors and/or inaccuracies in Personal Data no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives a request for updating and/or correction of Personal Data." Paragraph (2): "The Personal Data Controller shall notify the Personal Data Subject of the results of the update and/or correction of Personal Data."

Article 31: "The Personal Data Controller shall record all activities related to the processing of Personal Data."

Article 32 paragraph (1): "The Personal Data Controller shall provide the Data Subject with access to the Personal Data being processed along with the processing trail of the Personal Data in accordance with the storage period of the Personal Data." Paragraph (2): "The access referred to in paragraph (1) shall be provided no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives the access request."

Article 33: "The Personal Data Controller shall refuse to grant access to change Personal Data to the Personal Data Subject in the event that: a. it endangers the security, physical health, or mental health of the Personal Data Subject and/or other persons; b. it results in the disclosure of Personal Data belonging to other persons; and/or c. it conflicts with national defense and security interests."

Meanwhile, the rights of erasure and destruction are regulated in Articles 42 to 45, as follows (Republik Indonesia, 2022):

Article 42 paragraph (1): "The Personal Data Controller shall terminate the processing of Personal Data in the event that: a. the retention period has been reached; b. the purpose of processing Personal Data has been achieved; or c. there is a request from the Subject of Personal Data." Paragraph (2): "The termination of Personal Data processing as referred to in paragraph (1) shall be carried out in accordance with the provisions of laws and regulations."

Article 43 paragraph (1): "The Personal Data Controller shall delete Personal Data in the event that: a. Personal Data is no longer necessary for the achievement of the purpose of Personal Data processing; b. the Personal Data Subject has withdrawn consent for the processing of Personal Data; c. there is a request from the Personal Data Subject; or d. Personal Data is obtained and/or processed unlawfully." Paragraph (2): "The deletion of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions of laws and regulations."

Article 44 paragraph (1): "The Personal Data Controller shall destroy Personal Data in the event that: a. the retention period has expired and it is stated that it shall be destroyed based on the archive retention schedule; b. there is a request from the Personal Data Subject; c. it is not related to the settlement of a legal case; and/or d. Personal Data has been obtained and/or processed unlawfully." Paragraph (2): "The destruction of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions of laws and regulations."

Article 45: "The Personal Data Controller shall notify the Personal Data Subject of the deletion and/or destruction of Personal Data."

For public relations units, the implication is that any material that collects or displays personal data must have a mechanism to fulfill requests for access, correction, or deletion within the period specified by the PDP Law, as well as include information on the process of submitting such rights in public communications and privacy policies (Wachid et al., 2024).

The PDP Law also requires controllers to implement operational data protection principles, including the obligation to conduct a Data Protection Impact Assessment (DPIA) for high-risk processing, as well as technical and organizational obligations to maintain the security, confidentiality, and integrity of data ('Aisy et al., 2025; Mardyansyah et al., 2025). The provisions refer to Articles 34 to 39, as follows (Republik Indonesia, 2022):

Article 34 paragraph (1): "The Personal Data Controller shall conduct a Personal Data Protection impact assessment in cases where the processing of Personal Data has a high potential risk to the Personal Data Subject." Paragraph (2): "The processing of Personal Data that has a high potential risk as referred to in paragraph (1) includes: a. automated decision-making that has legal consequences or significant impact on the Data Subject; b. processing of specific Personal Data; c. processing of Personal Data on a large scale; d. processing of Personal Data for systematic evaluation, scoring, or monitoring activities of Personal Data Subjects; e. processing of Personal Data for matching or combining groups of data; f. use of new technology in the processing of Personal Data; and/or g. processing of Personal Data that restricts the exercise of the rights of Personal Data Subjects." Paragraph (3): "Further provisions regarding the assessment of the impact of Personal Data Protection are regulated in Government Regulations."

> Article 35: "The Personal Data Controller shall protect and ensure the security of the Personal Data it processes by: a. developing and implementing technical and operational measures to protect Personal Data from interference with the processing of Personal Data that is contrary to the provisions of laws and regulations; and b. determining the level of security of Personal Data by taking into account the nature and risks of the Personal Data that must be protected in the processing of Personal Data."
>
> Article 36: "In processing Personal Data, the Personal Data Controller shall maintain the confidentiality of Personal Data."
>
> Article 37: "The Personal Data Controller shall supervise every party involved in the processing of Personal Data under the control of the Personal Data Controller."
>
> Article 39 paragraph (1): "The Personal Data Controller shall prevent Personal Data from being accessed unlawfully." Paragraph (2): "The prevention referred to in paragraph (1) shall be carried out by using a security system for Personal Data that is processed and/or processing Personal Data using an electronic system that is reliable, secure, and responsible." Paragraph (3): "The prevention referred to in paragraph (2) shall be carried out in accordance with the provisions of laws and regulations."

In addition, Articles 40 to 41 regulate the termination, postponement, and restriction of processing if the subject withdraws their consent or files an objection (Republik Indonesia, 2022):

> Article 40 paragraph (1): "The Personal Data Controller shall cease processing Personal Data in the event that the Personal Data Subject withdraws their consent to the processing of Personal Data." Paragraph (2): "The cessation of Personal Data processing as referred to in paragraph (1) shall be carried out no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives the request to withdraw consent for the processing of Personal Data."
>
> Article 41 paragraph (1): "The Personal Data Controller shall be obliged to delay and restrict the processing of Personal Data, either partially or in whole, no later than 3 x 24 (three times twenty-four) hours from the time the Personal Data Controller receives the request for delay and restriction of the processing of Personal Data." Paragraph (2): "The suspension and restriction of Personal Data processing as referred to in paragraph (1) shall be exempted in the following cases: a. there are provisions in laws and regulations that do not allow the suspension and restriction of Personal Data processing; b. it may endanger the safety of other parties; and/or c. the Personal Data Subject is bound by a written agreement with the Personal Data Controller that does not allow for the postponement and restriction of Personal Data processing." Paragraph (3): "The Personal Data Controller shall notify the Personal Data Subject that the postponement and restriction of Personal Data processing has been carried out."

In the context of organizational communication, this provision requires the application of privacy by design in the campaign process, for example, risk assessment prior to the launch of a survey, retention policy audits prior to data redistribution, and internal procedures to stop processing if the subject's request is fulfilled (Alnajrani & Norman, 2020).

The division of roles between controllers and processors is also regulated in detail in Articles 51 to 52, which contain the obligations of processors to process only based on the instructions of the controller and the rules for the involvement of sub-processors, as well as the responsibilities if the processor acts outside of the instructions (Republik Indonesia, 2022):

> Article 51 paragraph (1): "In the event that the Personal Data Controller appoints a Personal Data Processor, the Personal Data Processor shall process Personal Data based on the instructions of the Personal Data Controller." Paragraph (2): "The processing of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the provisions set forth in this Law." Paragraph (3): "The processing of Personal Data as referred to in paragraph (1) is the responsibility of the Personal Data Controller." Paragraph (4): "The Personal Data Processor may involve other Personal Data Processors in the processing of Personal Data." Paragraph (5): "A Personal Data Processor must obtain written consent from the Personal Data Controller before involving another Personal Data Processor as referred to in paragraph (4)." Paragraph (6): "In the event that a Personal Data Processor processes Personal Data outside the orders and

purposes set by the Personal Data Controller, the processing of Personal Data shall be the responsibility of the Personal Data Processor."

Article 52: "The provisions regarding the obligations of the Personal Data Controller as referred to in Articles 29, 31, 35, 36, 37, 38, and 39 also apply to the Personal Data Processor."

The PDP Law further regulates the appointment of officials or officers who carry out data protection functions, often referred to as Data Protection Officers (DPOs), in Articles 53 to 56, with minimum duties including monitoring compliance and providing advice to controllers or processors. This applies to public relations professionals who work intensively with vendors, such as analytics platforms or advertising agencies (Sumandiyar et al., 2023). These articles require strict contractual clauses, written consent for sub-processors, and clear internal communication channels between the communications, legal, and DPO teams to ensure that each party understands the limits of processing. As stated in the articles (Republik Indonesia, 2022):

Article 53 paragraph (1): "Personal Data Controllers and Personal Data Processors shall appoint an official or officer to perform the function of Personal Data Protection in the following cases: a. processing of Personal Data for the purposes of public services; b. the core activities of the Personal Data Controller have a nature, scope, and/or purpose that requires regular and systematic monitoring of Personal Data on a large scale; and c. the core activities of the Personal Data Controller consist of the processing of Personal Data on a large scale for Personal Data that is specific in nature and/or Personal Data related to criminal acts." Paragraph (2): "Officials or officers who carry out the Personal Data Protection function as referred to in paragraph (1) shall be appointed based on their professionalism, knowledge of the law, Personal Data Protection practices, and ability to fulfill their duties." Paragraph (3): "Officials or officers who carry out the functions of Personal Data Protection as referred to in paragraph (2) may come from within and/or outside the Personal Data Controller or Personal Data Processor."

Article 54 paragraph (1): "Officials or officers who carry out Personal Data Protection functions have at least the following duties: a. to inform and advise Personal Data Controllers or Personal Data Processors to comply with the provisions of this Law; b. to monitor and ensure compliance with this Law -Law and the policies of the Personal Data Controller or Personal Data Processor; c. providing advice on the impact assessment of Personal Data Protection and monitoring the performance of the Personal Data Controller and Personal Data Processor; and d. coordinating and acting as a liaison for issues related to the processing of Personal Data." Paragraph (2): "In carrying out the duties referred to in paragraph (1), officials or officers performing Personal Data Protection functions shall take into account the risks associated with Personal Data processing, considering the nature, scope, context, and purpose of the processing." Paragraph (3): "Further provisions regarding officials or officers who carry out Personal Data Protection functions are regulated in Government Regulations."

Article 55 paragraph (1): "Personal Data Controllers may transfer Personal Data to other Personal Data Controllers within the jurisdiction of the Republic of Indonesia." Paragraph (2): "Personal Data Controllers who transfer Personal Data and those who receive transferred Personal Data shall be obliged to protect Personal Data as referred to in this Law."

Article 56 paragraph (1): "The Personal Data Controller may transfer Personal Data to Personal Data Controllers and/or Personal Data Processors outside the jurisdiction of the Republic of Indonesia in accordance with the provisions of this Law." Paragraph (2): "In transferring Personal Data as referred to in paragraph (1), the Personal Data Controller shall ensure that the country where the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data is located has a level of Personal Data Protection that is equivalent to or higher than that stipulated in this Law." Paragraph (3): "In the event that the provisions referred to in paragraph (2) are not met, the Personal Data Controller shall ensure that there is adequate and binding Personal Data Protection." Paragraph (4): In the event that the provisions referred to in paragraphs (2) and (3) are not met, the Personal Data Controller must obtain the consent of the Personal Data Subject. Paragraph (5): "Further provisions regarding the transfer of Personal Data are regulated in Government Regulations."

One key provision that has major implications for post-incident communication practices is the obligation to notify data subjects of breaches. Article 46 requires controllers to provide written notification within 3 x 24 hours to data subjects and relevant agencies, including minimum notification

content such as what data was exposed, when and how it was exposed, and mitigation efforts (Republik Indonesia, 2022). However, in reality, case studies and local research show a high frequency of breach incidents and problems in the implementation of notifications.

Many organizations choose to issue public media clarifications instead of direct notifications to subjects, thereby causing compliance and reputation problems. Research on personal data breach cases in Indonesia by Hartini et al. (2024) and Wibowo et al. (2024), as well as a fintech case study by Rohendi & Kharisma (2024) noted factors causing data leaks such as procedural weaknesses and third-party vendors, as well as the low level of incident response preparedness in many organizations, which makes the 72-hour obligation a practical challenge for public relations in designing legally and ethically compliant response messages.

Although the PDP Law has established a comprehensive normative framework, analysis shows a number of implementation gaps that are relevant to communication practices. *First*, the absence of detailed implementing regulations for several instruments, such as the DPIA mechanism and public notification standards, leaves room for interpretation by practitioners (Anggraini & Putra, 2025; Mardyansyah et al., 2025); *second*, the Constitutional Court's decision regarding the wording of certain articles, such as the interpretation of Article 53, adds to the normative uncertainty in the appointment of DPOs and their authority (Mahkamah Konstitusi, 2024); *third*, the literature recommends strengthening the autonomy and functional immunity of data protection officials so that they can advise communication teams without conflicts of interest (Wibowo et al., 2024). Therefore, public relations officers need to translate the provisions of the articles into operational SOPs, such as pre-campaign checklists, notification templates, and strict vendor contracts, while waiting for technical guidelines from the government and derivative regulations for implementation certainty.

4.2. Compliance of Communication Ethics Principles with Legal Provisions

The principle of informed consent in communication ethics requires valid, clear, and meaningful consent before data is collected or processed (Bisel & Mahutga, 2024; de Groot, 2024; van Goidsenhoven & de Schauwer, 2022). This is in line with Nissenbaum's (2004) idea that sharing norms must be context-appropriate (Contextual Integrity) so that consent must consider the relevant actors, attributes, and transmission principles. The PDP Law explicitly regulates the basis for processing, including consent, in Article 20 and outlines the obligation to provide information related to consent in Article 21 regarding the purpose, duration, recipients, etc. (Supeno et al., 2025; Syailendra et al., 2024). In public relations practice, ethical challenges arise when consent is formalistic without substantive information for the subject. A study by Çelik et al. (2025) highlights this practice as a real problem that reduces the quality of informed consent and calls for a reformulation of consent notifications to make them easier to understand.

Transparency is a key ethical principle that strengthens the autonomy of data subjects (Lee & Li, 2021), which is in line with Nissenbaum (2004) who emphasizes the relevance of the context of communication, and the PDP Law places the obligation of transparency in several articles, including Article 31 on the recording of processing activities, Article 32 on the access rights of subjects, a 3 x 24-hour time limit, and Article 21 on notification requirements for consent-based processing (Republik Indonesia, 2022). In practice, public relations must include data access and copying mechanisms in privacy policies and communication materials so that the public can verify processing (Wachid et al., 2024). Research by Khadafi et al. (2024) found that data leaks in Indonesia indicate a lack of transparency and delayed notifications exacerbate the reputational impact and risks for subjects. This reinforces the need to operationalize transparency in organizational communication SOPs.

Accountability as an ethical principle requires an accountable organizational structure (van Goidsenhoven & de Schauwer, 2022), such as the appointment of a DPO, processing logs, and audit mechanisms, all of which are accommodated by the PDP Law in Articles 31, 34, and Articles 51 to 56 relating to the appointment of data protection officers and the obligations of controllers and processors (Republik Indonesia, 2022). The theory of compliance and accountability shows that formal legal obligations are effective when supported by institutional capacity (Bisel & Mahutga, 2024). Articles and implementation guidelines emphasize the need for clear contractual clauses with vendors and internal oversight mechanisms so that public relations teams do not act independently without legal oversight or a DPO (Alexe & Şandru, 2021). The studies by Henriksen-Bulmer et al. (2020) dan van Landuyt et al.

(2020) on DPIA and its implementation practices provide evidence that organizations that internalize accountability are better able to respond to communication risks involving data.

The PDP Law normatively contains many provisions that are consistent with ethical principles of communication such as consent, transparency, accountability, and minimization, but analytical findings and empirical studies show a gap between formal compliance and operational practice (Syailendra et al., 2024; Widiatedja & Mishra, 2023). Several recent studies highlight implementation constraints, including the unclear functioning of the DPO ('Aisy et al., 2025), varied DPIA mechanisms (Anggraini & Putra, 2025), and incomplete implementing regulations for notification standards and consent templates (Triyanti et al., 2025; Wibowo et al., 2024). Therefore, ethical recommendations must complement the legal text. Public relations needs operational guidelines that translate the articles of the PDP Law into easy-to-follow and contextual practices that bridge law and ethics so that organizational communication is not only formally compliant but also ethically responsible.

4.3. Implementation Barriers and Ethical Dilemmas in Public Relations Practice

Various obstacles often encountered in the context of public relations are: *first*, institutional unpreparedness and weak resources to fulfill the obligations stipulated in the PDP Law, such as in Article 34 concerning the obligation to conduct a DPIA, Articles 35 to 39 concerning maintaining technical security, and meeting the deadline for notification of leaks in Article 46 (Republik Indonesia, 2022). Studies by Prabowo et al. (2025) and Anggraini & Putra (2025) show that there are still several public institutions that do not have the capability to conduct adequate DPIA or build the necessary recording and auditing systems, making legal obligations a heavy implementation burden. The findings of Syailendra et al. (2024) and other studies that inventory data breach cases confirm that budget constraints, a lack of experts, and unclear technical guidelines slow down the implementation of the operational obligations of the PDP Law (Abdillah et al., 2024; Hartini et al., 2024; Wibowo et al., 2024).

The second obstacle is the formalistic practice of consent and buried terms in privacy documents, a problem rooted in the gap between the principle of informed consent according to communication ethics and industry practices that prioritize administrative convenience over subject understanding (van Goidsenhoven & de Schauwer, 2022). Articles 20 to 21 of the PDP Law regulate the basis for processing and the information that must be provided (Republik Indonesia, 2022), but empirical research on leaks and literature analysis indicate that consent is often given through checkboxes without understandable explanations (de Groot, 2024), thus violating the spirit of contextual integrity according to Nissenbaum (2004, 2009). As a result, public relations often faces an ethical dilemma, namely meeting communication and marketing targets or postponing activities until meaningful consent is obtained, a choice that is risky for reputation and legal compliance.

The third obstacle relates to dependence on third parties, such as vendors, advertising platforms, or cloud providers, which complicates the controller's control over data flows (Georgiou & Lambrinoudakis, 2021; Søe & Mai, 2023). Articles 51 to 52 of the PDP Law regulate the division of roles and responsibilities between controllers and processors and require clear contracts with sub-processors (Republik Indonesia, 2022), but practice in the field shows that contracts are often inadequate or not effectively monitored. Case studies of national data breaches, such as those involving BPJS and financial institutions, reveal that vendor configuration weaknesses, cross-border data transfers without adequate protection, and sub-processors using other services have contributed to breaches (Admiral & Pauck, 2023; Algamar et al., 2024; Rohendi & Kharisma, 2024). This creates an ethical dilemma for communications teams: to what extent can they rely on vendors when ultimate responsibility remains with the controller? Best practices call for strict technical clauses and vendor audits, but this requires legal and technical capacities that not all organizations possess.

Furthermore, gaps in implementing regulations and legal uncertainty pose serious obstacles that result in varying interpretations by organizations. The PDP Law provides a general framework, but many operational provisions, including DPIA standards, incident notification formats, and processing risk thresholds, are still awaiting detailed derivative regulations (Amalia et al., 2022; Natamiharja & Setiawan, 2024; Syailendra et al., 2024). Literature gap analysis highlights how this void causes organizations to implement ad-hoc solutions, such as in the General Data Protection Rules (GDPR) in the European Union (Gleim et al., 2020), which may not be in line with the essence of the PDP Law. This uncertainty also raises ethical risks, such as public relations making communication decisions that

are semantically legal but less ethical in the context of data subject protection (Vuković et al., 2023; Wachid et al., 2024). Therefore, while the PDP Law establishes rights and obligations, such as the right of access or deletion, the effectiveness of protection is highly dependent on the issuance of practical and tested technical guidelines.

Another obstacle from the perspective of communication ethics and Solove's (2006) privacy damage map, is the practical dilemma when organizations must weigh public interest/corporate communication against individual privacy risks. For example, in cases of crisis reporting, marketing campaigns targeting vulnerable groups, or inter-agency data collaboration for public purposes (de Oliveira-Martins & Gonçalves-Sant'Ana, 2024; Devine, 2024). On the one hand, transparency and accountability, for example by providing relevant public information, are necessary (Lee & Li, 2021; Mager et al., 2025). On the other hand, the publication of erroneous data or summaries can lead to dissemination, discrimination, or invasion (Shimron et al., 2022). Therefore, internal decision-making mechanisms (ethics/data committees) involving public relations, legal, and DPOs are needed to assess trade-offs contextually and uphold the principle of non-maleficence.

4.4. Personal Data Protection in Other Countries: A Brief Comparison

To position Indonesia's PDP Law within the global landscape, this subsection presents a brief comparison of personal data protection frameworks in a number of countries and regions. This comparison highlights key legislation, the nature of regulatory approaches, and the practical implications for cross-jurisdictional organizational communications.

4.4.1. Malaysia, Singapore, and Philippines

Malaysia implements the Personal Data Protection Act 2010 (PDPA 2010), which regulates data processing in commercial transactions with a number of basic obligations such as access and correction rights. Malaysia's PDPA is older but still relevant domestically (Sholehuddin et al., 2024; Sudarwanto & Kharisma, 2022). Singapore has the Personal Data Protection Act (PDPA 2012) which, after several amendments, emphasizes the principle of organizational accountability and even has extraterritorial effects for activities involving Singaporean citizens or entities ('Aisy et al., 2025; Kharlie et al., 2025; Sholehuddin et al., 2024). The Philippines regulates through the Data Privacy Act of 2012 (DPA 2012), which established the National Privacy Commission (NPC) and requires breach notifications and governance standards for the public and private sectors (Amiludin et al., 2024; Sholehuddin et al., 2024). For public relations, these differences within ASEAN mean that notification requirements, contractual standards with vendors, and transparency expectations can vary between countries, so cross-border campaigns must be tailored accordingly.

4.4.2. South Korea and Japan

South Korea has enacted the Personal Information Protection Act (PIPA), which is one of the most stringent data protection regimes, explicit consent requirements for sensitive processing, cross-border transfer notification obligations, and active enforcement (Setiawati et al., 2020; Shin, 2021; Tsamara, 2021). Japan regulates through the Act on the Protection of Personal Information (APPI), which has undergone gradual amendments to strengthen the rights of subjects and introduce a monitoring mechanism by the Personal Information Protection Commission (PPC). The APPI focuses on balancing the use of data for innovation and the protection of individual rights (Oshima & Sakai, 2020; Pardieck, 2024; Tsamara, 2021). For communications practitioners, these two jurisdictions require campaign designs that pay close attention to the context of consent, data retention, and vendor control.

4.4.3. Ireland, France, and European Union

The European Union (EU), with its General Data Protection Regulation (GDPR), has established broad data protection standards: the principles of legality, limited purpose, strong subject rights, DPIA for risky processing, and cross-border transfer mechanisms (adequacy, SCC, BCR) (de Bruin, 2022; Tsamara, 2021). Ireland, through the Data Protection Act 2018 (DPA 2018), plays a crucial role as the lead regulator for many technology companies ('Aisy et al., 2025). France, with its *Commission Nationale de l'informatique et des Libertés* (CNIL) is known for its aggressive enforcement (Maat, 2022; Natamiharja & Setiawan, 2024). Both countries demonstrate that formal compliance is not sufficient if implementation is weak. The practical impact is that organizations conducting cross-EEA

communications must prioritize DPIA, legal documentation, and readiness for audits and potential large fines.

4.4.4. United Kingdom and Australia

The United Kingdom (UK) implemented the UK GDPR and Data Protection Act 2018 after Brexit (DPA after Brexit), with a regime that remains very similar to the GDPR but with domestic policy space; the Information Commissioner's Office (ICO) continues to enforce the rules and provide practical guidance (Erdos, 2023; Tsamara, 2021). Australia uses the Privacy Act 1988 (PA 1988), which regulates public entities and the majority of large businesses; recently, there has been a major review and a package of reform recommendations is underway to close modern loopholes (e.g., strengthening subject rights and enforcement) ('Aisy et al., 2025; Phillips, 2024). For public relations, it is important to understand the nuances (e.g., definition of regulated entities, revenue thresholds in Australia) and tailor privacy notices and incident response mechanisms according to jurisdiction.

4.4.5. China dan Hong Kong

China introduced the Personal Information Protection Law (PIPL), which resembles several elements of the GDPR (legal basis, subject rights, DPIA-like review, restrictions on cross-border transfers) but is combined with a focus on national security and strong state control—the PIPL contains heavy sanctions and strict data export rules (Calzada, 2022; Setiawati et al., 2020). Hong Kong has an older Personal Data (Privacy) Ordinance (PDPO) (1995) but it has been amended (e.g., anti-doxxing) and focuses on DPP principles. The PDPO is relatively more passive than the PIPL but still provides a practical framework for businesses (Sudarwanto & Kharisma, 2022; Tsamara, 2021). For organizational communications, the PIPL requires extra caution regarding data transfers, storage on domestic servers, and strict contractual compliance.

4.4.6. United States

The United States (US) does not have a single comprehensive federal law; its approach is sectoral (Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Children's Online Privacy Protection Act (COPPA), etc.) plus a growing number of comprehensive state laws—California leads with the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA), which grants rights of access, deletion, opt-out of data sale or rental, and the CPRA strengthens enforcement through the California Privacy Protection Agency (CPPA). As a result, global companies often adopt a combination of practices (de Bruin, 2022; Determann & Tam, 2020; Maharani et al., 2025; Tsamara, 2021). For public relations, the practical implication is the need for multi-layer compliance: meeting state requirements as well as federal sectoral rules, and maintaining nationally consistent documentation and incident response procedures.

Table 3. Comparison of Global Personal Data Protection

Country	Regulations	Characteristics	Implications for Organizational Communication
Malaysia	PDPA 2010	Focus on commercial transactions; fundamental rights of data subjects.	Notification and consent must be tailored to the business context.
Singapore	PDPA 2012	Organizational accountability, extraterritorial effects.	Concise privacy notice and strong internal governance.
Philippines	DPA 2012	Independent authority, incident notification.	Leak response readiness and communication documentation.
South Korea	PIPA	Highly protective, strict enforcement.	Explicit consent and strict vendor control.
Japan	APPI	Balance of innovation and protection.	Transparency of purpose and clear data retention.
Ireland	DPA 2018	Lead regulator for technology companies.	DPIA and crucial compliance documentation.
France	CNIL	Active enforcement and strict sanctions.	Accuracy of public messages and substantial compliance.

Australia	PA 1988	Entity thresholds, ongoing reform.	Cross-sector privacy policy adjustments.
China	PIPL	Strict, state control, cross-border transfers.	High caution on data exports and public messages.
Hong Kong	PDPO	Traditional principles, anti-doxxing.	Aggregation/anonymization in communication.
UK	UK GDPR + DPA after Brexit	Similar to post-Brexit GDPR.	DPIA compliance and ICO guidance.
EU	EU GDPR	Global standards, strong subject rights.	Global baseline for cross-border campaigns.
US	CCPA/CPRA	Patchwork, consumer focus.	Multi-layer compliance and clear opt-out.

Source: From Various Literature.

Broadly speaking, Indonesia's PDP Law has adopted a normative framework that is in line with international practices, such as recognition of data subject rights, division of roles between controllers and processors, DPIA obligations, and breach notification, so that in terms of design it resembles many of the principles applied in jurisdictions such as the EU or Singapore (Algamar et al., 2024; Sholehuddin et al., 2024). However, practical comparisons reveal important differences, namely that the EU through the GDPR and countries with established supervisory authorities excel in enforcement mechanisms, detailed technical guidelines, and deterrent fines (Maharani et al., 2025; Natamiharja & Setiawan, 2024).

On the other hand, some regimes such as China's PIPL emphasize cross-border controls and stricter data localization requirements (Calzada, 2022), while the US faces a federal-state patchwork (e.g., CPRA) that demands a multi-layer compliance strategy (Determann & Tam, 2020). Singapore and the Philippines stand out for their organizational accountability obligations and the active role of their private authorities (Amiludin et al., 2024; Kharlie et al., 2025). The implications for organizational communication practices in Indonesia are twofold: (1) The PDP Law provides a strong modern legal foundation for improving ethical practices (informed consent, transparency, minimization), but (2) its effectiveness will greatly depend on the issuance of technical regulations, enforcement capacity, and institutional readiness, areas in which lessons from the EU's GDPR, Singapore's PDPA, and China's PIPL can be used as adaptive references.

4.5. Ethical and Policy Recommendations

Operational recommendations for public relations units are to implement privacy by design in all communication activities, from the design of registration forms to post-campaign evaluation, with reference to the obligations of minimization and basic processing information (Articles 20–21 of the PDP Law) as well as technical or organizational obligations. Concrete practices include: (a) a concise privacy notice on every communication asset; (b) granular consent options (marketing vs. research); (c) a data breach notification template that complies with Article 46 of the PDP Law; and (d) a pre-campaign DPIA checklist to assess privacy risks.

These recommendations are supported by the theories of contextual integrity and privacy harms, which highlight the importance of contextualization and risk mitigation (Nissenbaum, 2009; Solove, 2006), as well as by empirical analyses of organizational readiness in Indonesia that highlight issues of formalistic consent and incident response readiness (Hartini et al., 2024; Wibowo et al., 2024). Internationally, DPIA practices and subject rights summaries in the EU GDPR, as well as organizational accountability principles in Singapore's PDPA, serve as useful technical references for solidifying these operational measures ('Aisy et al., 2025; Georgiou & Lambrinoudakis, 2021).

Recommendations for internal governance and vendor management with organizational measures must strengthen accountability structures by appointing independent data protection officers, establishing processing logs and internal audits, and strict contractual clauses for processors and sub-processors. Best practices include granting functional authority and immunity to DPOs to reject or review risky campaigns, audit rights over vendors, and data destruction provisions after the contract expires. Implementation studies in several ASEAN countries and analysis of leakage cases in the financial sector show that organizations that adopt strong governance and clear vendor clauses respond significantly faster to incidents and minimize reputational impact (Algamar et al., 2024; Sholehuddin et

al., 2024). The recommended operational policy is to implement a contract clause template that covers audit rights, purpose restrictions, and 24–72-hour incident notification, followed by SOPs for coordination between public relations, legal, and DPO, and periodic incident response drills.

Policy recommendations for national policymakers: expedite the issuance of implementing regulations detailing DPIA mechanisms, including risk threshold standards and report formats, practical data breach notification formats in accordance with Article 46, and technical security guidelines in Articles 35 to 39 of the PDP Law. In addition, strengthen the independent supervisory authority with enforcement capacity and resources, and issue sectoral guidelines (e.g., health, finance, education) that respond to specific sectoral public communication needs.

International lessons demonstrate the benefits of two things: (1) the EU GDPR exemplifies how DPIA and sanction mechanisms drive substantial compliance (Georgiou & Lambrinoudakis, 2021); (2) Singapore and Ireland exemplify the importance of practical guidelines and ease of regulator-industry collaboration ('Aisy et al., 2025). On the implementation side, transitional policies (capacity building for MSMEs, free templates, DPO training funding) will help close the resource gap identified in local studies. Finally, policy recommendations include harmonizing cross-border transfer mechanisms (SCC/adequacy style) to facilitate cross-border organizational communication without compromising data subject protection.

5. Conclusion

This study shows that the PDP Law in Indonesia has provided a comprehensive normative framework for regulating organizational communication practices, including the rights of subjects (Articles 30–45), the obligations of controllers or processors and contractual obligations (Articles 51–52), DPIA (Article 34), technical or organizational obligations (Articles 35–39), appointment of data protection officers (Articles 53–56) and breach notification (Article 46). However, findings show a gap between legal norms and operational practices: issues of formalistic consent, vendor dependency, institutional resource constraints, and unfinished implementing regulations pose implementation challenges and ethical dilemmas for public relations. Therefore, despite a strong legal foundation, the effectiveness of data protection in communication practices is highly dependent on the operationalization of contextual ethics and institutional capacity.

Practical advice and policies are as follows: at the organizational level, public relations must implement privacy by design by using a pre-campaign DPIA checklist (Article 34), a concise privacy notice and granular consent options (Articles 20–21), a 72-hour notification template (Article 46), and incident response SOPs involving the DPO/legal department. Strengthen vendor governance with strict contractual clauses (Articles 51–52) and periodic audits. At the public policy level, the government needs to immediately issue implementing regulations detailing DPIA standards, notification formats, and technical security guidelines (Articles 35–39), as well as strengthen supervisory authorities through resources and sectoral guidelines. In addition, capacity building programs (free templates, DPO training for MSMEs, practical guidelines for public relations) and cross-border transfer harmonization will accelerate compliance and close the gap between the law and ethical communication practices.

References

'Aisy, F. R., Maskur, M. A., & Amiruddin, A. . A. (2025). Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore. *Journal of Indonesian Legal Studies*, *10*(1), 431–482. https://doi.org/10.15294/jils.v10i1.13755

Abdillah, A., Widianingsih, I., Buchari, R. A., & Nurasa, H. (2024). Big data security & individual (psychological) resilience: A review of social media risks and lessons learned from Indonesia. *Array*, *21*, 100336. https://doi.org/10.1016/j.array.2024.100336

Admiral, A., & Pauck, M. A. (2023). Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services. *Lex Scientia Law Review*, *7*(2), 995–1048. https://doi.org/10.15294/lesrev.v7i2.77881

Alexe, I., & Şandru, D.-M. (2021). Data Protection in the Public Procurement Process. *European Journal of Law and Public Administration*, *7*(2), 224–239. https://doi.org/10.18662/eljpa/7.2/142

Algamar, M. D., Munir, A. B., & Hendro. (2024). Managing Indonesian Data Breach Notification in

the Financial Services Sector: A Case for One-Stop Notification Model. *Journal of Central Banking Law and Institutions*, *3*(3), 547–584. https://doi.org/10.21098/jcli.v3i3.271

Alnajrani, H. M., & Norman, A. A. (2020). The Effects of Applying Privacy by Design to Preserve Privacy and Personal Data Protection in Mobile Cloud Computing: An Exploratory Study. *Symmetry*, *12*(12), 2039. https://doi.org/10.3390/sym12122039

Amalia, C., Poetry, E. G., Kono, M. K., Kusuma, D. A., & Kurniawan, A. (2022). Legal Aspect of Personal Data Protection and Consumer Protection in the Open API Payment. *Journal of Central Banking Law and Institutions*, *1*(2), 323–352. https://doi.org/10.21098/jcli.v1i2.19

Amiludin, A., Nurhalisa, S., Umara, U. P., & Hidayatullah, H. (2024). Comparison of Protection Laws Private Data in Indonesia, and the Philippines. *Jurnal Jurisprudence*, *14*(2), 171–191. https://doi.org/10.23917/jurisprudence.v14i2.4266

Anggraini, D. I., & Putra, P. O. H. (2025). Data Protection Impact Assessment Framework in the Banking Sector in Indonesia to Implement Law of Personal Data Protection. *Jurnal Sistem Informasi*, *21*(1), 15–34. https://doi.org/10.21609/jsi.v21i1.1439

Ashby-King, D. T., Truban, O., & Lee, S. Y. (2025). Examining public relations practitioners' perceptions of authentic organizational social responsibility and advocacy communication. *Public Relations Review*, *51*(4), 102603. https://doi.org/10.1016/j.pubrev.2025.102603

Avanzi, B., Tan, X., Taylor, G., & Wong, B. (2025). On the Evolution of Data Breach Reporting Patterns and Frequency in the United States: A Cross-State Analysis. *North American Actuarial Journal*, *29*(4), 833–864. https://doi.org/10.1080/10920277.2025.2457491

Bisel, R. S., & Mahutga, J. (2024). Organizational Communication Ethics. In A. Pinchevski, P. M. Buzzanell, & J. Hannan (Eds.), *The Handbook of Communication Ethics* (2nd ed.). Routledge. https://doi.org/10.4324/9781003274506-14

Calzada, I. (2022). Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129–1150. https://doi.org/10.3390/smartcities5030057

Çelik, F., Koseoglu, M. A., & Ibrahim, B. (2025). Research on Corporate Social Responsibility in Public Relations: A Hybrid Review Through Topic Modeling Analysis and Way Forward. *Business Ethics, the Environment & Responsibility*, *34*(4), 2187–2209. https://doi.org/10.1111/beer.12762

Chapman, K., Smith, G., Klabacka, K., Winslow, H., Barkhuus, L., Faklaris, C., Das, S., Wisniewski, P., Knijnenburg, B. P., Lipford, H., & Page, X. (2025). Beyond the Legal Lens: A Sociotechnical Taxonomy of Lived Privacy Incidents and Harms. *ArXiv*, 1–33. https://arxiv.org/abs/2511.20791v1

Christou, P. A. (2022). How to use thematic analysis in qualitative research. *Journal of Qualitative Research in Tourism*, *3*(2), 79–95. https://doi.org/10.4337/jqrt.2023.0006

Croce, Y. Della. (2023). Epistemic Injustice and Nonmaleficence. *Journal of Bioethical Inquiry*, *20*(3), 447–456. https://doi.org/10.1007/s11673-023-10273-4

de Bruin, R. (2022). A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence. *UC Law Science and Technology Journal*, *13*(2), 127–166. https://repository.uclawsf.edu/hastings_science_technology_law_journal/vol13/iss2/4

de Groot, N. F. (2024). A contextual integrity approach to genomic information: what bioethics can learn from big data ethics. *Medicine, Health Care and Philosophy*, *27*(3), 367–379. https://doi.org/10.1007/s11019-024-10211-0

de Oliveira-Martins, D., & Gonçalves-Sant'Ana, R. C. (2024). Contextualizando a taxonomia da privacidade de Solove no ciclo de vida dos dados. *Comunicação Mídia e Consumo*, *21*(62), 558–580. https://doi.org/10.18568/cmc.v21i62.2873

Determann, L., & Tam, J. (2020). The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide. *Journal of Data Protection & Privacy*, *4*(1), 7–21. https://doi.org/10.69554/GCLK6627

Devine, J. W. (2024). The Political Privacy Dilemma: Private Lives and Public Office. *Journal of Applied Philosophy*, *41*(3), 391–408. https://doi.org/10.1111/japp.12683

Erdos, D. (2023). The UK GDPR, the Immigration Exception and Brexit: Interrogating Open Rights Group v Secretary of State for the Home Department and its Aftermath. *The Modern Law Review*, *86*(3), 785–800. https://doi.org/10.1111/1468-2230.12784

Fritz, J. M. H. (2022). Work/Life Relationships and Communication Ethics: An Exploratory

Examination. *Behavioral Sciences*, *12*(4), 104. https://doi.org/10.3390/bs12040104

Georgiou, D., & Lambrinoudakis, C. (2021). Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. *Future Internet*, *13*(3), 66. https://doi.org/10.3390/fi13030066

Gleim, L. C., Karim, M. R., Zimmermann, L., Kohlbacher, O., Stenzhorn, H., Decker, S., & Beyan, O. (2020). Enabling ad-hoc reuse of private data repositories through schema extraction. *Journal of Biomedical Semantics*, *11*(1), 6. https://doi.org/10.1186/s13326-020-00223-z

Görpe, T. S., & Öksüz, B. (2024). Perception and Contribution of Public Relations to Society: What Does the Public Think? Insights from Türkiye. *Social Sciences*, *13*(12), 675. https://doi.org/10.3390/socsci13120675

Hagelstein, J., Volk, S. C., Zerfass, A., Athaydes, A. S., Macnamara, J., Meng, J., & Hung-Baesecke, C.-J. F. (2024). Ethical Challenges of Digital Communication:A Comparative Study of Public Relations Practitioners in 52 Countries. *International Journal of Communication*, *18*, 1072–1093. https://ijoc.org/index.php/ijoc/article/view/20636

Hartini, R., Pramesti, Y. C., & Moh.Ali, H. (2024). Preventing Personal Data Misuse: Legal Protection in Online Loans. *Arena Hukum*, *17*(3), 732–755. https://doi.org/10.21776/ub.arenahukum2024.01703.12

Henriksen-Bulmer, J., Faily, S., & Jeary, S. (2020). DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems. *Future Internet*, *12*(5), 93. https://doi.org/10.3390/fi12050093

Imran, F., Shahzad, K., Butt, A., & Kantola, J. (2021). Digital Transformation of Industrial Organizations: Toward an Integrated Framework. *Journal of Change Management*, *21*(4), 451–479. https://doi.org/10.1080/14697017.2021.1929406

Khadafi, R., Nurmandi, A., Hasibuan, E. J., Harahap, M. S., Saputra, A., Mahardika, A., & Izharsyah, J. R. (2024). Assessing the Indonesian government's compliance with the public information disclosure law in the context of COVID-19 data transparency. *Frontiers in Political Science*, *6*. https://doi.org/10.3389/fpos.2024.1339506

Kharlie, A. T., Fathudin, F., Amny Azra, F. El, & Cheduerame, S. (2025). Comparative analysis of personal data protection in Indonesia and Singapore for a sustainable digital future. In M. D. H. Rahiem (Ed.), *Towards Resilient Societies: The Synergy of Religion, Education, Health, Science, and Technology* (1st ed., pp. 593–598). CRC Press. https://doi.org/10.1201/9781003645542-95

Kumar, P. C., Zimmer, M., & Vitak, J. (2024). A Roadmap for Applying the Contextual Integrity Framework in Qualitative Privacy Research. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1–29. https://doi.org/10.1145/3653710

Latifa, N. R. (2024, December 6). *Krisis Kebocoran Data Pribadi: Tata Kelola yang Buruk di Indonesia*. SiberMate. https://sibermate.com/hrmi/krisis-kebocoran-data-pribadi-tata-kelola-yang-buruk-di-indonesia

Lee, Y., & Li, J. Q. (2021). The role of communication transparency and organizational trust in publics' perceptions, attitudes and social distancing behaviour: A case study of the COVID-19 outbreak. *Journal of Contingencies and Crisis Management*, *29*(4), 368–384. https://doi.org/10.1111/1468-5973.12354

Li, J., Xiao, W., & Zhang, C. (2023). Data security crisis in universities: identification of key factors affecting data breach incidents. *Humanities and Social Sciences Communications*, *10*(1), 270. https://doi.org/10.1057/s41599-023-01757-0

Maat, E. P. (2022). Google v. CNIL: A Commentary on the Territorial Scope of the Right to Be Forgotten. *European Review of Private Law*, *30*(2), 241–262. https://doi.org/10.54648/erpl2022013

Mager, A., Eitenberger, M., Winter, J., Prainsack, B., Wendehorst, C., & Arora, P. (2025). Situated ethics: Ethical accountability of local perspectives in global AI ethics. *Media, Culture & Society*, *47*(5), 1028–1041. https://doi.org/10.1177/01634437251328200

Maharani, D. P., Kusumadara, A., Widhiyanti, H. N., & Dewantara, R. (2025). Revisiting personal data: Ownership theories and comparative legal perspectives from Europe, Indonesia and the United States. *Journal of Data Protection & Privacy*, *7*(3), 274–291. https://doi.org/10.69554/ZMLG9061

Mahkamah Konstitusi. (2024). *Putusan Nomor 151/PUU-XXII/2024*.

Mardyansyah, D. N., Sukarmi, S., Kusumaningrum, A., & Widyanti, Y. E. (2025). Harmonization of Personal Data Protection Principles With Electronic Justice Systems In Indonesia. *Yuridika*, *40*(3), 343–368. https://doi.org/10.20473/ydk.v40i3.74179

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

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, *79*(1), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Oshima, Y., & Sakai, M. (2020). The Enforcement of Personal Data Protection Law in Japan. *Global Privacy Law Review*, *1*(3), 173–179. https://doi.org/10.54648/GPLR2020094

Pardieck, A. M. (2024). Privacy Matters: Data Breach Litigation in Japan. *Washington International Law Journal*, *33*(1), 1–43. https://digitalcommons.law.uw.edu/wilj/vol33/iss1/3

Paul, J., Ueno, A., Dennis, C., Alamanos, E., Curtis, L., Foroudi, P., Kacprzak, A., Kunz, W. H., Liu, J., Marvi, R., Nair, S. L. S., Ozdemir, O., Pantano, E., Papadopoulos, T., Petit, O., Tyagi, S., & Wirtz, J. (2024). Digital transformation: A multidisciplinary perspective and future research agenda. *International Journal of Consumer Studies*, *48*(2), e13015. https://doi.org/10.1111/ijcs.13015

Phillips, J. (2024). How does the consent model in Australia's Privacy Act 1988 (Cth) undermine our human right to privacy? *Australian Journal of Human Rights*, *30*(3), 329–348. https://doi.org/10.1080/1323238X.2024.2418558

Prabowo, S., Abdurohman, M., Nuha, H. H., & Sutikno, S. (2025). Identifying and Validating Critical Factors in Designing a Comprehensive Data Protection Impact Assessment (DPIA) Framework for Indonesia. *International Journal of Safety and Security Engineering*, *15*(1), 113–126. https://doi.org/10.18280/ijsse.150113

Rabitti, G., Khorrami Chokami, A., Coyle, P., & Cohen, R. D. (2025). A taxonomy of cyber risk taxonomies. *Risk Analysis*, *45*(2), 376–386. https://doi.org/10.1111/risa.16629

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Rohendi, A., & Kharisma, D. B. (2024). Personal data protection in fintech: A case study from Indonesia. *Journal of Infrastructure, Policy and Development*, *8*(7), 4158. https://doi.org/10.24294/jipd.v8i7.4158

Rushagama, F. M. (2024). Combined Doctrinal and Qualitative Approach in Legal Researches: An over view. *International Journal of Innovative Science and Research Technology*, *9*(1), 1780–1785. https://doi.org/10.5281/zenodo.10634265

Santos, K. da S., Ribeiro, M. C., Queiroga, D. E. U. de, Silva, I. A. P. da, & Ferreira, S. M. S. (2020). O uso de triangulação múltipla como estratégia de validação em um estudo qualitativo. *Ciência & Saúde Coletiva*, *25*(2), 655–664. https://doi.org/10.1590/1413-81232020252.12302018

Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, *2*(2), 95–109. https://doi.org/10.18196/iclr.2219

Shaya, M. F., & Ahmad, J. (2024). Navigating the transformation through the insights from a study on public relations and organisational transformation. *Cogent Social Sciences*, *10*(1). https://doi.org/10.1080/23311886.2024.2306753

Shimron, E., Tamir, J. I., Wang, K., & Lustig, M. (2022). Implicit data crimes: Machine learning bias arising from misuse of public data. *Proceedings of the National Academy of Sciences*, *119*(13), e2117203119. https://doi.org/10.1073/pnas.2117203119

Shin, S.-Y. (2021). Privacy Protection and Data Utilization. *Healthcare Informatics Research*, *27*(1), 1–2. https://doi.org/10.4258/hir.2021.27.1.1

Sholehuddin, N., Miskam, S., Mohd Shahwahid, F., Raja Abdul Aziz, T. N., & Mansor, N. (2024). A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries. *Journal of Muwafaqat*, *7*(1), 23–38. https://doi.org/10.53840/muwafaqat.v7i1.166

Søe, S. O., & Mai, J.-E. (2023). The Ethics of Sharing: Privacy, Data, and Common Goods. *Digital Society*, *2*(2), 28. https://doi.org/10.1007/s44206-023-00057-z

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560. https://doi.org/10.2307/40041279

Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, *29*(4), 1443–1457. https://doi.org/10.1108/JFC-09-2021-0193

Sumandiyar, A., Smith, J. C. M., Syahr, Z. H. A., Husain, M. N., & Suharyanto, A. (2023). Influencer relations: the new paradigm of public relations. *Jurnal Studi Komunikasi (Indonesian Journal of*

Communications Studies), *7*(2), 401–416. https://doi.org/10.25139/jsk.v7i2.6688

Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal Data Protection in Review of Legal Theories and Principles. *Journal of Law and Legal Reform*, *6*(3), 1349–1376. https://doi.org/10.15294/jllr.v6i3.10252

Sutherland, K., Freberg, K., Driver, C., & Khattab, U. (2020). Public relations and customer service: Employer perspectives of social media proficiency. *Public Relations Review*, *46*(4), 101954. https://doi.org/10.1016/j.pubrev.2020.101954

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, *14*(2), 56–72. https://doi.org/10.15742/ilrev.v14n2.4

Toruan, R. C. L. (2025, July 30). *Polemik Data Pribadi: 5 Kasus Kebocoran Data di Indonesia Selama 2023-2024*. TEMPO. https://www.tempo.co/digital/polemik-data-pribadi-5-kasus-kebocoran-data-di-indonesia-selama-2023-2024-2052924

Triyanti, N., Handayani, I. G. A. K. R., & Karjoko, L. (2025). Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law. *Hasanuddin Law Review*, *11*(1), 132–147. https://doi.org/10.20956/halrev.v11i1.6177

Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, *3*(1), 53–85. https://doi.org/10.26740/jsh.v3n1.p53-84

van Goidsenhoven, L., & de Schauwer, E. (2022). Relational ethics, informed consent, and informed assent in participatory research with children with complex communication needs. *Developmental Medicine & Child Neurology*, *64*(11), 1323–1329. https://doi.org/10.1111/dmcn.15297

van Landuyt, D., Sion, L., Dewitte, P., & Joosen, W. (2020). The Bigger Picture: Approaches to Inter-organizational Data Protection Impact Assessment. In I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, & A. Sasse (Eds.), *Lecture Notes in Computer Science* (pp. 283–293). Springer Cham. https://doi.org/10.1007/978-3-030-66504-3_17

Vuković, M., Dašić, D., & Vuković, A. (2023). Ethical and legal aspects of Public relations. *Pravo - Teorija i Praksa*, *40*(4), 93–111. https://doi.org/10.5937/ptp2304093V

Wachid, I. B., Wulandari, M. P., & Nasution, Z. (2024). Navigating ethical challenges in Indonesian digital public relations practices. *Bricolage : Jurnal Magister Ilmu Komunikasi*, *10*(2), 267–282. https://doi.org/10.30813/bricolage.v10i2.5478

Wasserman, H. (2024). Media accountability and ethics in Africa. In M. Puppis, R. Mansell, & H. van den Bulck (Eds.), *Handbook of Media and Communication Governance* (pp. 274–284). Edward Elgar Publishing. https://doi.org/10.4337/9781800887206.00031

White, M. G., & Koskey, A. F. (2025, August 22). *Ten Key Insights from IBM's Cost of a Data Breach Report 2025*. Baker Donelson. https://www.bakerdonelson.com/ten-key-insights-from-ibms-cost-of-a-data-breach-report-2025

Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, *10*(1). https://doi.org/10.1080/23311886.2024.2306751

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

Yourell, J. L., McAlister, K. L., Beatty, C. C., & Huberty, J. L. (2025). Exploring Ethics: Understanding the Role of Privacy Policies and Institutional Review Boards in Digital Health Companies. *Journal of Medical Internet Research*, *27*, e70711–e70711. https://doi.org/10.2196/70711

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., & Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. *International Journal of Information and Computer Security*, *19*(3–4), 402–442. https://doi.org/10.1504/IJICS.2022.127169