

Constitutionalizing Personal Data Protection in Indonesia: Reframing Privacy, State Responsibility, and Digital Governance

First Author^{1*}, Second Author², Third Author³, Fourth Author⁴, Fourth Author⁵

Institution/University¹, Institution/University², Institution/University³, Institution/University⁴, Institution/University⁵

ORCID: [https://orcid.org/...] for each author, where available

*Corresponding Author's E-mail: (for the first author only)

Article History	Received (date/month/year)	Revised (date/month/year)	Accepted (date/month/year)
-----------------	-------------------------------	------------------------------	-------------------------------

Article Info

Abstract

The rapid digitization of public administration, commerce, communication, and identity systems has transformed personal data from an administrative resource into a constitutional governance issue. Indonesia has responded through Law Number 27 of 2022 on Personal Data Protection (PDP Law), which expressly connects personal data protection with the constitutional protection of personal self under Article 28G paragraph (1) of the 1945 Constitution. Yet the existence of statutory rights does not by itself settle the constitutional questions generated by large-scale data processing, state access, public-interest disclosures, automated decision-making, and institutional accountability. This article examines how personal data protection can be reconstructed as a constitutional obligation within Indonesia's digital governance framework. It asks three questions: how Article 28G and related constitutional rights ground personal data protection; whether the PDP Law provides an adequate architecture for translating constitutional rights into institutional duties; and what constitutional accountability model can reconcile privacy, public information, and legitimate governmental functions. The study employs normative legal research using statutory, conceptual, comparative, and case approaches. Primary materials include the 1945 Constitution, the PDP Law, and Constitutional Court Decision Number 135/PUU-XXIII/2025, while secondary materials include international human-rights instruments and scholarship on privacy and digital constitutionalism. The analysis proposes a four-dimensional Constitutional Data Accountability Model consisting of legality, necessity and proportionality, institutional accountability, and effective remedy. The model treats data protection not merely as regulatory compliance but as a continuing constitutional duty that should guide legislation, administration, judicial review, and digital-system design.

Keywords:

Constitutional Rights;
Digital Constitutionalism;
Indonesia
Personal Data;
Privacy;
Proportionality;
State Responsibility;

To cite this article: Author names. (2026). "Constitutionalizing Personal Data Protection in Indonesia: Reframing Privacy, State Responsibility, and Digital Governance" *NUCLA: Nusantara Constitutional Law*, Volume 1, Issue 1, December 2026; Page: 1 – 22.



This article is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)©2026 by author/s

1. INTRODUCTION

1.1 Background and Problem Context

Digital transformation has altered the constitutional environment in which individuals exercise rights and public authorities exercise power. Identification, authentication, social

protection, taxation, health services, education, banking, mobility, and communication increasingly depend on the collection and processing of information that can identify or profile individuals. The constitutional significance of this transformation lies not simply in the volume of information held by institutions, but in the capacity to aggregate information across contexts, infer characteristics, automate decisions, and affect opportunities without direct physical intervention. Digital constitutionalism therefore concerns not only whether a state may regulate the Internet, but also how constitutional values are preserved when data infrastructures become part of the machinery of governance ([De Gregorio & Radu, 2022](#)).

In Indonesia, the constitutional foundation for privacy is most directly located in Article 28G paragraph (1) of the 1945 Constitution, which guarantees protection of personal self, family, honor, dignity, possessions, security, and freedom from threats to act or refrain from acting. Article 28F additionally protects the right to communicate and obtain information, while Article 28J establishes that the exercise of rights may be limited by law for legitimate purposes within a constitutional framework. The constitutional structure consequently contains both a protective dimension and a balancing dimension. Personal data protection must protect individuals against arbitrary interference while also accommodating information access, public administration, law enforcement, and other constitutionally legitimate functions.

Law Number 27 of 2022 on Personal Data Protection represents a major statutory development. Its explanatory section expressly characterizes personal data protection as connected to the protection of personal self and identifies Article 28G paragraph (1), Article 28H paragraph (4), and Article 28J as constitutional foundations. The statute regulates principles, categories of data, data-subject rights, processing, controller and processor obligations, transfers, sanctions, institutions, dispute resolution, prohibited conduct, and criminal provisions (Law No. 27/2022). The official regulatory database records that the law entered into force on 17 October 2022 and remains in force.

The emergence of this framework, however, does not eliminate constitutional uncertainty. A statutory regime can recognize rights while still leaving difficult questions about how those rights operate when the state itself becomes a data controller, when information is disclosed in the public interest, when data processing is automated, or when multiple public bodies share information. Recent scholarship has consequently shifted from asking whether privacy exists to examining institutional responsibility, proportionality, remedies, and the relationship between privacy and other constitutional rights ([Beduschi, 2021](#)).

1.2 Research Gap

Existing Indonesian scholarship has established several important propositions. First, Article 28G is a constitutional basis for privacy and personal data protection ([Fauzi & Radika Shandy, 2022](#); [Rahman & Wicaksono, 2021](#)). Second, the PDP Law provides a more coherent legal framework than the previously fragmented sectoral regime. Third, digital government creates special challenges because the state may simultaneously regulate data, collect data, process data, and provide remedies. Recent studies have also begun to examine constitutional proportionality and Constitutional Court adjudication in the digital context ([Charity & Anshory, 2026](#)). These contributions provide an important foundation, but they leave room for a more integrated constitutional model that connects substantive rights, processing rules, institutional design, and remedies.

The gap is therefore analytical rather than merely descriptive. Many discussions treat personal data protection as a branch of administrative or technology law and constitutional protection as a general normative justification. This separation can obscure the fact that data processing decisions are exercises of public and private power with

consequences for autonomy, dignity, equality, expression, and participation. Digital constitutionalism scholarship emphasizes that digital infrastructures reorganize relationships between individuals, states, and private actors. The relevant constitutional question is consequently how constitutional constraints travel through the entire data lifecycle—from collection and purpose specification to sharing, retention, automated use, disclosure, and remedy ([De Gregorio & Radu, 2022](#)).

This article addresses that gap by treating the PDP Law as an implementation instrument of constitutional rights rather than as a self-contained regulatory code. The argument is that constitutional adequacy should be assessed through four connected dimensions: a lawful basis for processing; necessity and proportionality of interference; institutional accountability for those who control data; and accessible remedies when rights are violated. The model is intended to be applicable to both state and non-state processing, while giving special attention to public authorities because constitutional obligations are most directly engaged when the state exercises coercive or administrative power.

1.3 Research Questions and Objectives

The study addresses three research questions. *First*, how should Article 28G paragraph (1), together with Articles 28F and 28J, be interpreted as the constitutional foundation of personal data protection in Indonesia? *Second*, to what extent does the PDP Law translate that constitutional foundation into substantive, procedural, and institutional safeguards? *Third*, what constitutional accountability model can guide the reconciliation of privacy, information rights, public administration, and legitimate state interests in digital governance?

The objectives are correspondingly threefold: to reconstruct the constitutional meaning of personal data protection; to assess the statutory architecture of rights, duties, exceptions, institutions, and remedies; and to formulate a normative model that can assist legislators, administrators, courts, and digital-system designers in applying constitutional standards throughout the data lifecycle.

1.4 Research Significance and Contribution

The article contributes a constitutional accountability framework rather than another inventory of PDP Law provisions. Its principal contribution is the Constitutional Data Accountability Model, which connects legality, necessity and proportionality, institutional accountability, and remedy into a single evaluative sequence. The model is designed to prevent a common analytical error: treating compliance with a statutory procedure as sufficient evidence of constitutional legitimacy. The framework instead asks whether the legal basis is sufficiently clear, whether the interference is genuinely necessary, whether safeguards and oversight are institutionally independent and effective, and whether affected persons can obtain correction, cessation, compensation, or judicial review where appropriate.

2. LITERATURE REVIEW

Privacy scholarship has long resisted a single, exhaustive definition of privacy. Solove (2006) argues that privacy problems take multiple forms, including information collection, processing, dissemination, and invasion, and that legal analysis benefits from a taxonomy capable of identifying concrete harms. His later work similarly treats privacy as a plural and contextual concept rather than a simple right to secrecy ([Solove, 2006](#)). This approach is particularly useful for personal data because a person may experience harm

even when individual data points are publicly observable. Aggregation, inference, profiling, secondary use, and dissemination can alter the meaning and consequences of information.

Bennett and Raab (2006) place privacy within a broader governance perspective. They emphasize that privacy protection is shaped by policy instruments, institutional arrangements, regulation, self-regulation, and technological measures. This perspective helps explain why a rights-based statute may underperform if supervisory institutions lack sufficient authority, expertise, coordination, or accountability. Personal data protection is therefore a governance system, not simply a prohibition on disclosure.

Human-rights scholarship has increasingly linked privacy with dignity, autonomy, equality, expression, and participation. The United Nations Human Rights Council has repeatedly affirmed that the same rights people have offline must also be protected online and that unlawful or arbitrary surveillance and data collection may interfere with privacy and other human rights (United Nations Human Rights Council [UNHRC], 2021, 2023). The 2024 report of the Special Rapporteur on the right to privacy further emphasizes legal safeguards for personal data and privacy in the digital age (Nougrères, 2024). These international materials are not substitutes for Indonesian constitutional interpretation, but they provide relevant interpretive context for understanding the minimum logic of legality, necessity, proportionality, and effective safeguards.

Digital constitutionalism provides the bridge between privacy law and constitutional governance. De Gregorio and Radu (De Gregorio & Radu, 2022) describe digital technologies as infrastructures through which rights and power are exercised. Internet governance increasingly involves hybrid arrangements in which public and private actors jointly shape the conditions under which rights can be exercised. This observation is important for Indonesia because the PDP Law regulates controllers and processors that may include governmental and private entities. A constitutional approach must therefore address both vertical power between state and citizen and horizontal power between data subjects and powerful data-processing organizations.

Indonesian literature confirms the relevance of this synthesis. Rahman and Wicaksono (Fauzi & Radika Shandy, 2022; Rahman & Wicaksono, 2021) examine the constitutional reference for interpreting personal data and identify Article 28G as a central foundation. Fauzy and Shandy (2023) connect the right to privacy with the legal politics of the PDP Law. More recent research emphasizes state responsibility and the need for institutional accountability in digital government (Wiredarme, 2025; Reni et al., 2026). The present article builds on these strands by organizing them into a single constitutional accountability sequence rather than treating each issue separately.

3. THEORETICAL AND CONCEPTUAL FRAMEWORK

3.1 Theoretical Framework

The first theoretical pillar is constitutional rights theory. A constitutional right is not exhausted by a formal prohibition against interference; it can also generate positive duties to establish institutions, procedures, safeguards, and remedies. In the context of personal data, the state therefore has at least three types of responsibility: to respect privacy by refraining from arbitrary processing, to protect individuals from harmful processing by private or public actors, and to fulfill rights through institutions and procedures that make protection effective. This tripartite logic is consistent with the broader human-rights understanding of privacy in the digital age (UNHRC, 2021, 2024).

The second pillar is proportionality. Article 28J requires rights limitations to be based on law and directed toward constitutionally legitimate objectives. Proportionality provides a

structured method for examining whether an interference is suitable, necessary, and appropriately balanced. In data governance, proportionality is especially relevant because the existence of a legitimate governmental purpose does not automatically justify the collection of all available information. The constitutional inquiry must distinguish between what the state wants to achieve and what amount or type of data processing is genuinely required to achieve it.

The third pillar is digital constitutionalism. Digital constitutionalism is used here not as a new constitution but as a field of constitutional reasoning concerned with how rights and limits on power operate in digital environments. Digital systems can redistribute power by making information asymmetries permanent, scalable, and difficult for individuals to observe. This means constitutionalism must reach the architecture of decision-making, not merely the final administrative decision. Transparency, auditability, human oversight, and contestability become constitutional governance concerns when automated systems affect rights.

3.2 Conceptual Framework

The conceptual framework treats the data lifecycle as the object of constitutional accountability. The lifecycle begins with collection and legal basis, continues through purpose specification and processing, extends to sharing and transfer, and ends with retention, deletion, or further use. At every stage, four questions should be asked: Is there a valid legal basis? Is the processing necessary and proportionate? Who is accountable and subject to meaningful oversight? What remedy exists if the person is harmed?

Table 1. Conceptual Framework Flow

Dimension	Core Constitutional Question	Indicative Safeguards
Legality	Is the interference authorized by clear and accessible law?	Defined purpose; lawful basis; clear authority; notice
Necessity & proportionality	Is the processing necessary and appropriately limited?	Data minimization; purpose limitation; balancing; impact assessment
Institutional accountability	Who decides, audits, supervises, and answers for the processing?	DPO/PPDP; supervisory institution; audit trails; independent review
Effective remedy	Can the affected person challenge, correct, stop, or obtain redress?	Access; correction; complaint; dispute resolution; judicial review; compensation

Source: Data processed by the author from various sources, 2026.

The framework differs from a purely compliance-oriented model because it evaluates the relationship between rules and constitutional purposes. A technically compliant system may still be constitutionally problematic if its legal basis is vague, its data collection is excessive, its oversight is dependent on the institution being supervised, or its remedies are practically inaccessible. Conversely, a well-designed system can translate constitutional values into operational controls before harm occurs.

3.3 Analytical Matrix

The model can be operationalized as a matrix for legislation, administrative programs, judicial review, and organizational governance. The matrix does not create new legal obligations by itself. Instead, it provides an interpretive structure for assessing whether existing obligations are being implemented in a manner consistent with constitutional rights. This distinction is important for a normative legal article: the model is a scholarly

proposal for organizing legal reasoning, not a claim that the four dimensions already constitute a formally enacted Indonesian test.

Table 2. Analysis Matrix

Stage	Primary Inquiry	Evidence to Examine	Possible Constitutional Risk
Collection	Why is data collected and under what authority?	Law, regulation, consent, public-service mandate	Arbitrary or excessive collection
Processing	What is done with the data and for what purpose?	Processing records, policies, algorithms	Function creep; incompatible secondary use
Sharing/transfer	Who receives data and why?	Agreements, legal basis, transfer safeguards	Uncontrolled dissemination
Automated decision-making	How does data affect an individual?	Models, decision rules, human review	Opacity, discrimination, inability to contest
Retention/deletion	How long is data retained and why?	Retention schedule, deletion logs	Permanent exposure and repurposing
Remedy	How can a person challenge misuse?	Complaint channels, decisions, judicial review	Formal rights without effective relief

Source: Data processed by the author from various sources, 2026.

This matrix responds to a central feature of digital governance: harm can arise without a single dramatic act of disclosure. A data subject may suffer through repeated collection, cross-database linkage, profiling, inaccurate inference, or inability to correct a record. Solove’s taxonomy is useful here because it shifts attention from the binary question of secrecy to the broader ecology of privacy harms (Solove, 2006).

The framework also accommodates legitimate public interests. Personal data may be processed for public services, legal obligations, vital interests, public interest, or other lawful purposes recognized by the PDP Law. The constitutional issue is not whether public purposes are inherently illegitimate, but whether the chosen processing is legally authorized, connected to the stated purpose, appropriately limited, and surrounded by safeguards. The government’s own explanation in Constitutional Court proceedings concerning Articles 65(2) and 67(2) illustrates this balancing problem: the state argued that personal data protection should coexist with public information and professional activities, rather than automatically displacing them (Ministry of Communication and Digital Affairs, 2025).

The framework consequently treats rights balancing as a continuous process. A legal basis is the threshold condition, proportionality limits the intensity of processing, institutional accountability distributes responsibility, and remedy completes the constitutional cycle. The four dimensions are interdependent. Weakness in one dimension can undermine the others. For example, a broad legal basis combined with weak oversight can permit excessive processing; strong oversight without accessible remedies can leave individuals unable to challenge errors; and detailed rights without transparent decision-making can make those rights difficult to exercise.

4. METHODOLOGY

4.1 Research Design and Approach

This study uses normative legal research with statutory, conceptual, comparative, and case approaches. Normative research is appropriate because the central questions concern the meaning, coherence, and constitutional adequacy of legal norms rather than

the measurement of individual attitudes or the incidence of data breaches. The analysis reconstructs relationships among constitutional provisions, statutory duties, institutional arrangements, and judicial reasoning. It does not claim to measure the actual compliance rate of Indonesian data controllers.

4.2 Sources of Data/Legal Materials

Primary legal materials consist of the 1945 Constitution of the Republic of Indonesia; Law Number 27 of 2022 on Personal Data Protection; and Constitutional Court Decision Number 135/PUU-XXIII/2025. The latter is relevant because the case challenged Articles 65(2) and 67(2) of the PDP Law in relation to constitutional rights including the rights in Articles 28C(1), 28F, and 32(1). The official JDIH record states that the case was decided on 19 January 2026 and the Court rejected the petition in its entirety.

Secondary materials include peer-reviewed scholarship on constitutional privacy, digital constitutionalism, data governance, proportionality, and digital identity, as well as United Nations reports and resolutions addressing privacy in the digital age. Particular attention is given to scholarship that directly examines Indonesia's constitutional framework, including Rahman and Wicaksono (Fauzi & Radika Shandy, 2022; Rahman & Wicaksono, 2021), Fauzy and Shandy (Fauzi & Radika Shandy, 2022; Rahman & Wicaksono, 2021), Wiredarme (2025), Reni et al. (2026), and Charity and Anshory (2026). International materials are used as comparative and interpretive resources rather than as directly binding Indonesian law.

4.3 Selection Criteria

Materials were selected when they satisfied at least one of four criteria: they establish the constitutional or statutory framework; they interpret privacy and data protection as human rights; they address digital constitutionalism or institutional accountability; or they analyze a relevant Indonesian judicial development. Sources that merely describe technological trends without legal implications were not treated as central authorities.

4.4 Research Procedure and Analysis

The research proceeded through four analytical stages. *First*, constitutional provisions were mapped against statutory principles and rights. *Second*, the PDP Law was examined as a governance architecture, focusing on legal bases, rights of data subjects, obligations of controllers and processors, exceptions, institutional functions, sanctions, and remedies. *Third*, Constitutional Court Decision Number 135/PUU-XXIII/2025 was examined as a contemporary illustration of tension between data protection and information-related constitutional interests. Fourth, the findings were synthesized through the proposed four-dimensional Constitutional Data Accountability Model.

4.5 Research Rigor and Ethics

Because the study uses publicly available legal and scholarly materials and does not involve human participants, it does not require human-subject ethical approval. Rigor is maintained through source triangulation: constitutional text is checked against statutory provisions, official legal databases, the Constitutional Court record, and scholarly interpretation. Where a source reports a contested position, the position is attributed to the relevant actor rather than presented as an uncontested fact.

5. RESULTS

5.1 The Constitutional Basis of Personal Data Protection

The first finding is that personal data protection has a constitutional foundation even though the 1945 Constitution does not use the phrase “personal data” as a standalone right. Article 28G paragraph (1) protects personal self, family, honor, dignity, possessions, and security. In a digital environment, personal data can constitute a practical extension of personal self because it enables institutions to identify, classify, predict, and act upon individuals. The constitutional meaning of “personal self” therefore should not be frozen in a pre-digital understanding of physical intrusion.

Article 28F creates a complementary constitutional interest. Individuals have a right to communicate and obtain information through available channels. This protects the circulation of information that is essential to democratic participation, education, public accountability, and social interaction. Personal data protection cannot therefore be conceptualized as an absolute entitlement to suppress information. The constitutional task is to distinguish legitimate information flows from unjustified exposure of personal information.

Article 28J provides the structural mechanism for reconciling these rights. Restrictions must be established by law and directed to purposes recognized by the Constitution, while respecting morality, religious values, security, and public order in a democratic society. For data governance, this suggests a three-step constitutional inquiry: the legal basis must be sufficiently clear; the purpose must be legitimate; and the interference must remain within the limits necessary to achieve that purpose.

The statutory framework reinforces this constitutional reading. The official explanation of the PDP Law expressly states that personal data protection is a human-rights concern and identifies Article 28G paragraph (1), Article 28H paragraph (4), and Article 28J among its constitutional foundations. The law therefore does not invent the constitutional interest from nothing; it concretizes an existing constitutional protection into rights, duties, procedures, and sanctions.

This finding supports a rights-centered interpretation of the PDP Law. Where a provision is ambiguous, interpretation should prefer a reading that preserves the constitutional protection of personal self while also respecting other constitutional rights. Such interpretation is particularly important where criminal sanctions or administrative powers are involved, because constitutional legality requires clear and predictable rules. The result is not an absolute hierarchy in which privacy always prevails, but a structured constitutional relationship in which competing rights and public purposes must be justified.

5.2 The Statutory Architecture of the PDP Law

The second finding is that the PDP Law has a comparatively comprehensive architecture. It regulates principles, data categories, data-subject rights, processing, controllers and processors, cross-border transfers, sanctions, institutional arrangements, dispute resolution, prohibited conduct, and criminal liability. The official legal database describes the law as covering both administrative and criminal dimensions and expressly links protection of personal data to constitutional rights.

The law also recognizes multiple legal bases for processing. The official materials concerning the Constitutional Court proceedings identify six bases under Article 20(2): valid consent; contractual necessity; legal obligation; vital interests; public interest or public service; and other legitimate interests subject to purpose, necessity, and balancing considerations. This architecture is significant because it prevents consent from becoming

the only conceptual foundation of lawful processing. Public administration frequently relies on statutory authority rather than freely negotiable consent.

The rights of data subjects and the obligations of controllers and processors create a corresponding structure of accountability. The law provides duties concerning processing, security, notification, and the appointment of personnel responsible for data protection functions in specified circumstances. The official JDIH material identifies Article 53 as requiring a data-protection officer or function for public-service processing and certain large-scale or sensitive processing activities.

The institutional chapter is particularly important. Article 58 states that the government's personal-data-protection function is carried out by an institution established by the President, while Article 59 assigns policy, supervision, administrative enforcement, and alternative dispute-resolution functions. Article 60 further enumerates supervisory and enforcement powers.

The architecture is therefore broad, but breadth does not automatically establish constitutional adequacy. The key question becomes how the statutory components operate together. Rights without independent oversight may be difficult to enforce. Legal bases without clear purpose limitation may permit function creep. Administrative sanctions without effective complaints may not provide individual redress. Conversely, criminal sanctions without sufficiently precise application may create uncertainty for legitimate information activities. The constitutional accountability model is designed to test these interactions rather than assess each provision in isolation.

5.3 Institutional Accountability and the State as Data Controller

Digital government changes the constitutional position of the state. In conventional administrative law, the state primarily issues decisions and delivers services. In digital administration, it increasingly performs these functions through databases, interoperable systems, identity infrastructures, analytics, and automated processes. The state can therefore become a collector, controller, processor, sharer, and beneficiary of personal data. This concentration of informational power increases the importance of institutional accountability.

The PDP Law's institutional chapter recognizes the need for a dedicated institutional function. Article 58 provides that the relevant institution is established by the President and is responsible to the President, while Article 59 gives it policy, supervision, administrative enforcement, and dispute-facilitation responsibilities. The institutional design must consequently be assessed not only in terms of formal authority but also in terms of independence, expertise, transparency, procedural fairness, and capacity to investigate powerful controllers.

Recent official policy developments illustrate that institutional design remains an active governance issue. In July 2026, the Ministry of Communication and Digital Affairs reported that the government was finalizing a plan for an independent personal-data-protection authority. The announcement described the proposed institution as independent in its work while reporting through the ministry to the President. This policy development demonstrates that statutory recognition of an institution and the operational realization of that institution are distinct stages of legal governance.

From a constitutional perspective, accountability should operate vertically and horizontally. Vertical accountability means that a data subject can challenge state processing through administrative and judicial channels. Horizontal accountability means that internal organizational controls, professional data-protection functions, audit trails, and supervisory review prevent a single administrative unit from exercising unchecked

informational power. The latter is particularly relevant where decisions are automated or datasets are shared across agencies.

The state's constitutional responsibility should therefore be understood as a chain of duties: establish lawful processing authority; define purpose and limits; minimize unnecessary data; secure information; document processing; supervise subordinate bodies and service providers; notify and respond to breaches; provide accessible complaints; and ensure judicial review where constitutional rights are implicated. This is consistent with the broader proposition that data privacy protection requires more than substantive rights—it requires institutions capable of making those rights effective (Reni et al., 2026; Wiredarme, 2025).

5.4 Rights Balancing, Public Information, and the 2026 Constitutional Court Decision

A particularly useful contemporary case is Constitutional Court Decision Number 135/PUU-XXIII/2025, decided on 19 January 2026. The case concerned Articles 65(2) and 67(2) of the PDP Law and was brought by applicants including an academic, an illustrator, the Alliance of Independent Journalists, and SAFEnet. The constitutional provisions invoked included Articles 28C(1), 28F, and 32(1). The official JDIH record states that the Court rejected the petition in its entirety.

The case illustrates a central constitutional tension: personal data protection may intersect with freedom of expression, information access, journalism, academic activity, and artistic work. The applicants argued that the challenged provisions could create uncertainty because professional activities may involve the disclosure of personal information in the public interest. During the proceedings, government representatives maintained that the provisions were intended to ensure lawful disclosure and were not designed to close legitimate journalistic, academic, or artistic activity.

The case is analytically important even without treating it as a universal formula. It demonstrates that privacy protection must coexist with other constitutional rights. A data-protection rule should not be interpreted as a blanket prohibition on information. At the same time, a public-interest label cannot automatically eliminate the privacy interests of data subjects. The relevant constitutional inquiry is whether the disclosure has a lawful basis, serves a legitimate public purpose, uses the minimum information necessary, and contains safeguards against irrelevant or harmful exposure.

The government's submissions during the proceedings identified Article 20(2) legal bases and emphasized that processing should comply with principles of data protection. This supports the first two dimensions of the proposed model: legality and necessity/proportionality. The case also demonstrates why remedies and institutional accountability matter. When a rule is applied to journalists, academics, researchers, or public-interest actors, the affected party needs a predictable mechanism for determining whether a disclosure is lawful before criminal liability is imposed.

The constitutional significance of the case therefore extends beyond its outcome. It provides an example of the need for rights-sensitive interpretation of data-protection provisions. Privacy and information rights should be treated as mutually constraining constitutional interests. The objective is not to declare one right categorically superior, but to develop legal standards capable of distinguishing justified disclosure from arbitrary dissemination.

5.5 Exceptions, Necessity, and the Risk of Function Creep

A recurring constitutional challenge in digital governance is the expansion of data use beyond the purpose for which information was initially collected. A database created for public services may later become attractive for law enforcement, eligibility screening, behavioral analytics, or inter-agency profiling. Each additional use may be administratively convenient, but convenience is not identical to constitutional necessity. Purpose limitation is therefore a constitutional safeguard against function creep.

The PDP Law recognizes several grounds for processing, including legal obligations, public interest, public services, and legitimate interests. The existence of these grounds is important for functional government, but the grounds must be read together with purpose, necessity, and balancing requirements. The official government explanation submitted in the 135/PUU-XXIII/2025 proceedings specifically describes legitimate-interest processing as subject to purpose, necessity, and balance between controller interests and data-subject rights.

Exceptions also require heightened scrutiny when they concern national security, law enforcement, or other public interests. Article 50 of the PDP Law provides exclusions from specified controller obligations for certain purposes, including national defense and security, law enforcement, public interest in state administration, and financial-sector oversight. Such provisions serve legitimate governmental functions, but from a constitutional perspective the existence of an exception should not mean the disappearance of all safeguards. Exceptions should remain connected to legality, purpose, necessity, institutional authorization, security, and remedy to the extent compatible with the function being performed.

This is where proportionality becomes operational. Suppose an agency has a legitimate objective of preventing fraud. The constitutional question is not simply whether fraud prevention is legitimate. It is whether the specific dataset, retention period, linkage method, profiling technique, and sharing arrangement are necessary for that objective and whether less intrusive alternatives exist. A broad data demand may be suitable in a general sense but still disproportionate if a narrower dataset would achieve the same result.

The same reasoning applies to automated decision-making. If an algorithm uses personal data to determine eligibility, risk, or access to services, the constitutional interest extends beyond confidentiality. Individuals may need an explanation, an opportunity to correct inaccurate data, and a meaningful channel for human review. Beduschi (2021) similarly emphasizes that digital identity systems should integrate privacy and human-rights considerations throughout the identity lifecycle, not merely at the point of data collection.

6. DISCUSSION

6.1 From Privacy Protection to Digital Constitutionalism

The results indicate that Indonesia's PDP framework should be understood as part of a broader constitutional transformation. Digital constitutionalism does not replace constitutional law; it asks how constitutional principles operate when digital systems mediate the exercise of rights and governmental power. De Gregorio and Radu (De Gregorio & Radu, 2022) identify fragmentation, polarization, and hybridization as major features of contemporary Internet governance. These features matter for privacy because data processing frequently crosses institutional, sectoral, and territorial boundaries.

The constitutional significance of personal data therefore has at least three layers. The first is individual: data can reveal identity, relationships, location, health, finances, beliefs, and behavior. The second is institutional: databases allow organizations to classify and make

decisions about individuals. The third is systemic: large-scale data infrastructures can shape access to services, political participation, economic opportunity, and social visibility. A constitutional framework focused only on confidentiality addresses the first layer but may miss the institutional and systemic dimensions.

The proposed model responds by treating data governance as a form of power that requires justification. Legality constrains the source of power. Proportionality constrains its intensity. Institutional accountability constrains its exercise. Remedy constrains its consequences. This structure resembles classical constitutionalism, but its object has expanded from legislation and administrative decisions to information infrastructures and data-processing systems.

This approach also clarifies the role of private actors. When a private platform controls data essential to communication, employment, finance, or public services, its decisions can affect the practical enjoyment of rights even though the actor is not formally part of the state. The PDP Law's application to controllers and processors provides a statutory bridge. Constitutional values should inform interpretation, while sectoral regulators and courts can ensure that contractual or technological power does not become a substitute for lawful authority.

The result is a more relational conception of privacy. Privacy is not merely an individual demand for secrecy but a condition for autonomy, dignity, equality, and participation. This is consistent with Solove's pluralistic understanding of privacy harms and with international human-rights materials emphasizing that digital privacy supports the enjoyment of other rights ([Solove, 2006](#); [UNHRC, 2021](#)). The constitutional protection of data should therefore be assessed according to the effects of processing on human agency, not merely according to whether information was technically disclosed.

6.2 Proportionality as a Bridge between Privacy and Public Interest

The central practical contribution of the framework is to position proportionality between constitutional recognition and administrative implementation. Public authorities often possess legitimate reasons to process data. Citizens also possess legitimate interests in privacy, security, autonomy, and information control. The legal problem is therefore one of structured reconciliation rather than simple prohibition.

The first proportionality question is suitability: can the proposed processing plausibly contribute to the stated objective? A measure that collects extensive personal data but has no meaningful relationship to the objective fails at the first stage. The second is necessity: is there a less intrusive measure that would achieve the same objective with comparable effectiveness? The third is balancing: do the benefits of the processing justify the rights burden after considering safeguards and affected interests?

These questions should be documented before high-risk processing begins. Data-protection impact assessments can serve this function. Beduschi (2021) recommends integrating impact assessment and privacy by design into digital identity systems. In Indonesia, the statutory requirement for data-protection functions and the broader obligations of controllers provide a foundation for operationalizing this logic. The constitutional value of impact assessment lies not in paperwork but in forcing decision-makers to confront rights implications before deployment.

Proportionality also has a procedural dimension. A decision may be substantively justified but procedurally defective if the individual has no opportunity to understand or challenge it. Transparency should therefore be calibrated to the nature of the processing. Not every technical detail can be publicly disclosed, particularly where security is involved, but affected persons should receive enough information to exercise their rights. The same

principle applies to automated decisions: secrecy about proprietary systems should not automatically eliminate meaningful contestability.

The proportionality approach also helps interpret criminal provisions. Where the PDP Law imposes criminal sanctions for unlawful disclosure, the principle of legality requires clear boundaries between punishable misuse and legitimate activity. The Constitutional Court proceedings demonstrate the importance of this issue because applicants connected the challenged provisions to journalism, information, academic activity, and artistic expression. The constitutional objective should be to protect data subjects without creating an indeterminate criminal standard that discourages lawful public-interest activity.

6.3 Comparative and International Lessons

International standards provide useful reference points for the Indonesian framework. The United Nations has repeatedly recognized privacy in the digital age as a human-rights concern and has emphasized that arbitrary or unlawful surveillance and data collection can interfere with privacy and other rights. The 2021 Human Rights Council resolution reaffirmed privacy protections in digital environments, while the 2023 resolution continued this line of institutional attention.

The 2024 report of the Special Rapporteur on the right to privacy focuses specifically on legal safeguards for personal data protection. It highlights the need for domestic legal frameworks capable of responding to technological developments and institutional power. These materials support the proposition that data protection should not be reduced to commercial consumer regulation. It is connected to the exercise of fundamental rights and requires effective legal remedies.

Comparative experience also suggests that institutional design matters. Data protection regimes commonly combine substantive principles with supervisory institutions, accountability mechanisms, impact assessments, and individual rights. Bennett and Raab (2006) demonstrate that privacy governance involves an interaction among law, regulation, institutional capacity, self-regulation, and technology. The lesson for Indonesia is not to copy another jurisdiction mechanically, but to ensure that statutory rights are supported by institutional mechanisms capable of enforcing them.

The Indonesian framework already contains several of these components. It identifies lawful bases, rights of data subjects, controller and processor duties, data-protection functions, administrative and criminal sanctions, and institutional responsibilities. The remaining constitutional task is to integrate these components through a consistent standard of justification. The proposed model can therefore be viewed as a method of harmonization rather than a new regulatory regime.

Comparative analysis also cautions against over-centralization. Strong supervision is necessary, but constitutional accountability should not depend exclusively on one executive institution. Courts, legislatures, internal compliance functions, professional data-protection officers, public-information mechanisms, civil-society organizations, and individuals should each have a role. A plural accountability system reduces the risk that data governance becomes a closed administrative domain.

For Indonesia, the most transferable principle is consequently not a specific institutional structure but a governance logic: rights must be enforceable against the institutions that process data; restrictions must be legally grounded and proportionate; supervisory power must be reviewable; and individuals must have practical remedies. This logic is compatible with the constitutional structure of Indonesia while remaining responsive to global digital-rights developments.

6.4 The Proposed Constitutional Data Accountability Model

The article proposes the Constitutional Data Accountability Model (CDAM) as the main scholarly contribution. CDAM consists of four sequential but mutually reinforcing dimensions. The first dimension is legality. Every significant processing activity should be traceable to a recognized legal basis and a defined purpose. The second is necessity and proportionality. The controller should demonstrate why the processing is required, why the volume and type of data are appropriate, and what safeguards reduce rights impacts. The third is institutional accountability. Responsibility should be allocated to identifiable decision-makers and supported by internal and external oversight. The fourth is effective remedy. Individuals should be able to know, challenge, correct, stop, or obtain redress for unlawful or harmful processing within the limits established by law.

Table 3. Proposes the Constitutional Data Accountability Model

CDAM Dimension	Minimum Normative Requirement	Institutional Output
Legality	Clear authority, defined purpose, lawful basis, accessible rules	Processing register and legal-basis record
Necessity & proportionality	Purpose limitation, minimization, risk assessment, balancing	Impact assessment and justification record
Institutional accountability	Named controller, DPO/PPDP function, audit, supervision	Audit trail, compliance report, supervisory decision
Effective remedy	Access, correction, objection/complaint, dispute resolution, judicial review	Complaint record, corrective action, compensation or other remedy

Source: Data processed by the author from various sources, 2026.

The model can be applied prospectively and retrospectively. Prospectively, a public agency designing a digital service should identify the legal basis, purpose, data categories, risks, safeguards, responsible officials, and remedies before deployment. Retrospectively, a court or supervisory authority examining a disputed processing activity can ask whether each dimension was satisfied. This dual application makes the model useful for both governance and adjudication.

CDAM also introduces a distinction between formal and substantive accountability. Formal accountability asks whether a required document or procedure exists. Substantive accountability asks whether the procedure meaningfully protects rights. A data-protection impact assessment that merely reproduces generic language may satisfy a formal requirement but fail substantive review. Similarly, a complaint channel that cannot correct records or suspend harmful processing may exist institutionally but provide weak remedy.

The model is deliberately technology-neutral. It can apply to databases, digital identity systems, artificial intelligence, biometric processing, cloud services, public-sector analytics, and conventional record systems. This is important because constitutional principles should remain stable even as technology changes. Specific technical standards may evolve, but the questions of legality, necessity, accountability, and remedy remain relevant.

The model also provides a practical bridge between constitutional adjudication and administrative governance. Courts can use it to structure proportionality analysis; legislators can use it when drafting statutory safeguards; agencies can use it for program design; and data controllers can use it for compliance. In this sense, the contribution is not to expand constitutional doctrine beyond recognition but to make existing constitutional commitments operational within data-intensive governance.

7. STUDY LIMITATIONS

This study has several limitations. *First*, it is normative and does not measure actual compliance by Indonesian ministries, agencies, courts, private platforms, or other data controllers. The proposed model should therefore be treated as a framework for legal evaluation rather than evidence of implementation outcomes. *Second*, the comparative component is selective and primarily serves interpretive purposes; it does not constitute a systematic comparative study of all major data-protection jurisdictions. *Third*, Constitutional Court Decision Number 135/PUU-XXIII/2025 is analyzed as an illustrative case of rights balancing rather than as a complete reconstruction of Indonesian privacy jurisprudence. *Fourth*, the article does not examine confidential government databases, proprietary algorithms, or individual breach investigations. These limitations create opportunities for empirical research on institutional implementation, judicial practice, and the effectiveness of remedies.

8. NOVELTY AND SCHOLARLY CONTRIBUTION

The novelty of this article lies in the formulation of the Constitutional Data Accountability Model, which integrates four dimensions—legality, necessity and proportionality, institutional accountability, and effective remedy—into a single constitutional framework for personal data governance. Existing Indonesian studies have established the constitutional basis of privacy, examined the PDP Law, or analyzed particular tensions between data protection and expression. This article extends those discussions by proposing a lifecycle-oriented framework that connects constitutional principles to the operational stages of data processing. The contribution is therefore both doctrinal and governance-oriented: it offers a method for interpreting existing law and a structured tool for assessing institutional design.

9. CONCLUSION AND IMPLICATIONS

9.1 Conclusion

The study finds that personal data protection in Indonesia should be understood as a constitutional obligation grounded principally in Article 28G paragraph (1), while remaining structurally connected to Article 28F and the limitation framework of Article 28J. The PDP Law translates this constitutional foundation into a comprehensive statutory architecture of rights, lawful bases, controller and processor duties, institutional functions, sanctions, and remedies. Nevertheless, constitutional adequacy depends on how these components operate together. Data protection cannot be reduced to secrecy, consent, or administrative compliance because digital processing can affect autonomy, dignity, equality, expression, and participation.

The analysis of Constitutional Court Decision Number 135/PUU-XXIII/2025 demonstrates the importance of balancing privacy with information-related constitutional interests. The decision does not eliminate the need for interpretive standards; rather, it illustrates why lawful disclosure, public interest, professional activity, and personal data protection must be evaluated through structured legal reasoning. The proposed CDAM provides that structure by requiring legality, necessity and proportionality, institutional accountability, and effective remedy across the data lifecycle.

9.2 Theoretical and Doctrinal Implications

Theoretically, the article advances a relational understanding of privacy within digital constitutionalism. Doctrinally, it suggests that Article 28G should be interpreted

dynamically so that “personal self” encompasses the informational conditions through which individuals are identified, classified, and governed. This interpretation does not create an unlimited constitutional right to control all information; it requires context-sensitive justification whenever data processing significantly affects protected interests.

9.3 Policy and Practical Implications

For policymakers and public authorities, the principal implication is that digital programs should embed constitutional accountability before deployment. Legal-basis records, purpose limitation, minimization, impact assessment, audit trails, responsible officers, supervisory review, and effective complaint mechanisms should be treated as elements of constitutional governance rather than optional compliance practices. Institutional design should also ensure that supervisory functions are sufficiently authoritative, professional, transparent, and subject to legal review.

9.4 Recommendations and Future Research

Future research should empirically test CDAM in public-service systems, digital identity, health information, social assistance, taxation, and artificial-intelligence decision-making. Comparative studies could examine how Indonesian constitutional doctrine interacts with different supervisory models and cross-border data-transfer regimes. Judicial studies should also trace whether proportionality reasoning becomes more explicit in future Constitutional Court and administrative-court decisions concerning personal data. These studies would allow the proposed normative model to be refined through evidence from institutional practice.

10. DECLARATIONS

10.1 Author Contributions

Author 1 conceptualized the study, developed the research questions and theoretical framework, conducted the legal analysis, and drafted the manuscript. Author 2 contributed to the literature review, comparative analysis, interpretation of legal materials, and critical revision of the manuscript. Both authors reviewed the final version, approved the submitted manuscript, and accept responsibility for the integrity of the work. The contribution statement follows the logic of the **CRedit** taxonomy and may be adapted to the journal’s required format.

10.2 Funding (if any)

This illustrative manuscript received no specific external funding. For an actual submission, authors should disclose all institutional, grant, project, or other financial support in accordance with the target journal’s policy.

10.3 Conflict of Interest

The authors declare no competing financial or non-financial interests that could have influenced the analysis presented in this manuscript.

10.4 Ethics Approval and Consent

The study used publicly available legal documents, court materials, legislation, international instruments, and scholarly publications and did not involve human participants or identifiable private research data. Ethical approval and informed consent were therefore not applicable.

10.5 Data and Materials Availability

The legal and scholarly materials analyzed in this study are publicly accessible through official legal databases, the Constitutional Court, United Nations documentation, and scholarly journal platforms. No proprietary dataset was generated for the study.

10.6 Acknowledgments

The authors acknowledge the public legal-information institutions and scholarly repositories that make constitutional, statutory, judicial, and international materials accessible for academic research.

REFERENCES

- Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.
- Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, 3, e15. <https://doi.org/10.1017/dap.2021.15>
- Charity, M. L., & Anshory, S. (2026). Balancing Constitutional Rights and Personal Data Protection for Citizens in the Digital Society: A Proportionality Test Analysis of Constitutional Court Decisions. *Indonesian Journal of Digital Society Is a Scientific Journal*, 2(1), 37–48. <https://doi.org/10.47313/.v2i1.4351>
- De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, 30(1), 68–87. <https://doi.org/10.1093/ijlit/eaac004>
- Fauzi, E., & Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Lex Renaissance*, 7(3), 445–461. <https://doi.org/10.20885/JLR.vol7.iss3.art1>
- Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection. State Gazette of the Republic of Indonesia 2022 Number 196, Supplement Number 6820.
- Mahkamah Konstitusi Republik Indonesia. (2026). Constitutional Court Decision Number 135/PUU-XXIII/2025, decided 19 January 2026.
- Nougrères, A. B. (2024). Legal safeguards for personal data protection and privacy in the digital age. Report of the Special Rapporteur on the Right to Privacy, A/HRC/55/46. United Nations Human Rights Council.
- Rahman, F., & Wicaksono, D. A. (2021). Researching References on Interpretation of Personal Data in the Indonesian Constitution. *Jurnal Penelitian Hukum De Jure*, 21(2), 187–200. <https://doi.org/10.30641/dejure.2021.V21.187-200>

- Reni, W. O., Syahbudin, & Momo, A. H. (2026). State responsibility and constitutional protection of personal data in Indonesia: Addressing digital challenges. *Kanun: Jurnal Ilmu Hukum*, 27(3), 706–726. <https://doi.org/10.24815/kjih.v27i3.139>
- Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477. <https://doi.org/10.2307/40041279>
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- United Nations Human Rights Council. (2021). The right to privacy in the digital age: Resolution A/HRC/RES/48/4.
- United Nations Human Rights Council. (2023). The right to privacy in the digital age: Resolution A/HRC/RES/54/21.
- United Nations Human Rights Council. (2024). Legal safeguards for personal data protection and privacy in the digital age: Report A/HRC/55/46.
- Wiredarme. (2025). Tanggung jawab konstitusional negara terhadap perlindungan data pribadi warga dalam penyelenggaraan pemerintahan digital. *Jurnal Perlindungan Masyarakat: Bestuur Praesidium*.
- Kementerian Komunikasi dan Digital Republik Indonesia. (2025). Keterangan pemerintah dalam perkara pengujian Pasal 65 ayat (2) dan Pasal 67 ayat (2) UU PDP, Perkara Nomor 135/PUU-XXIII/2025.
- Kementerian Komunikasi dan Digital Republik Indonesia. (2026, July 22). Wamen Nezar Patria: Indonesia siapkan otoritas perlindungan data pribadi yang independen.