RUMAH JURNAL ILMIAH MULTIDISIPLIN
E-ISSN: 3124-4408

==========

Harmonizing Public Information Disclosure and Personal Data Protection in Government Procurement Following LKPP Head Decision Number 129 of 2025

Siti Afifah[1], Nasywa Novita Sari[2], Zaskia Najwa Azzahra[3], Hiltsa Mutiara Ramadhani[4]
[1-4] Constitutional Law Study Program, Faculty of Sharia, State Islamic University of Palangka Raya
Email: fifahfifah2812@gmail.com[1] , nasywanovitasari22@gmail.com[2] , zaskiaazzahra420@gmail.com[3] , hiltsamr@gmail.com[4]

Abstract
Government procurement digitalization expands public access to contract, provider, and budget information, yet it also increases risks of exposing personal data in procurement documents and electronic systems. The problem arises because previous studies examine procurement transparency and personal data protection separately, while implications of LKPP Head Decision Number 129 of 2025 remain rarely analyzed in an integrated manner. This study asks how disclosure limits should operate after the decision and aims to formulate proportional harmonization between transparency and personal data protection. A normative legal method was applied through regulatory inventory, classification of primary and secondary legal materials, policy review, and prescriptive qualitative analysis of open and exempt information. Findings show that core information, including procurement plans, winners, contract values, funding sources, and work progress, remains open, while detailed owner estimates, technical bids, partnership agreements, and identities are restricted because of competition, privacy, and security risks. Consequently, harmonization requires phased disclosure, consequence testing, personal-data redaction, and restricted access to sensitive information.
Keywords: *information disclosure; personal data protection; government procurement; legal harmonization.*

INTRODUCTION

Government goods/services procurement occupies an important position in public administration because it is directly connected with the use of public budgets, service delivery, infrastructure development, and the fulfillment of administrative needs of the state. The digitalization of procurement through the Electronic Procurement System (SPSE), the General Procurement Plan Information System (SiRUP), the Electronic Catalog, and the INAPROC ecosystem has expanded opportunities for the public to monitor how public funds are spent. Such disclosure performs a strategic function because information on planning, provider selection, contract values, and work outputs enables the public to assess the accountability of procurement administrators. The official government procurement training module likewise places transparency, openness, competition, fairness, efficiency, and accountability among the principal elements of procurement governance (Baihaki & Rachman, 2022).

The issue becomes more complex when procurement information disclosure intersects with the growing use of digital data belonging to providers, procurement officials, experts, business-entity personnel, and other parties whose information appears in procurement documents. Such data may include identities, signatures, addresses, contact numbers, financial information, business-administration documents, and information relating to technical strategies and commercial interests. The enactment of Law Number 27 of 2022 on Personal Data Protection introduced new obligations requiring data processing and disclosure to have a lawful basis and to respect the rights of data subjects. This development places procurement governance under two legal demands at the same time: the public requires adequate information to oversee budget utilization, while parties whose data appear in procurement documents have a legal interest in the confidentiality and security of their personal data (Budhijanto, 2024).

The interaction between these two interests received a more concrete regulatory form through LKPP Head Decision Number 129 of 2025 concerning the List of Public Information and the List of Exempt Information in Government Goods/Services Procurement. The Decision regulates information from the planning stage through the handover of completed work and provides that the General Procurement Plan is disclosed through SiRUP, while other public procurement information is, in principle, accessible after the work or procurement process has been completed. At the same time, the Decision classifies several categories as exempt information, including procurement documents that are confidential by nature, details of the Owner's Estimate (HPS), design drawings, technical bids, responses

to objections, responses to appeal objections, partnership agreement letters, and bidder identities in e-reverse auctions. In particular, the Personal Data Protection Act is cited as one of the legal grounds for exempting partnership agreement letters because disclosure may reveal private information. Bidder identities in e-reverse auctions are likewise classified as exempt to protect data relating to individual or entity participants (LKPP, 2025a).

Social facts demonstrate that demands for procurement information disclosure remain relevant because digitalization has not always produced uniformly complete information. In electronic procurement in West Nusa Tenggara, for example, 13 procurement packages during 2017-2020 recorded corrected bid values of IDR 0, even though the combined budget ceiling of those packages reached IDR 54,620,180,375. The same study identified 76 goods-procurement packages in which tenders failed without adequate explanations of the reasons for failure, as well as 76 packages during 2017-2018 that did not identify the winning companies (Rifaid & Zulkarnain, 2021). These conditions demonstrate a concrete need for complete procurement information. However, legal developments following the enactment of the Personal Data Protection Act require demands for document disclosure to be accompanied by an assessment of which data may properly be published, which parts should be redacted, and which information has a lawful basis for restriction.

Previous literature shows a progression from the issue of transparency toward broader information-governance concerns. Rifaid and Zulkarnain (2021) found that e-procurement provides public access, yet incomplete information concerning tender processes remains a problem, meaning that procedural transparency is not always accompanied by adequate informational transparency. Resminingayu (2022) examined public participation in procurement-transparency commitments through the Open Government Partnership and showed that opening procurement data can strengthen public oversight when the government, LKPP, the Information Commission, and civil society have clearly defined spaces for collaboration. Manurung and Thalib (2023) drew attention to another dimension of technology use: the increasing risk of personal-data misuse arising from the collection, storage, and dissemination of data through digital systems, making the Personal Data Protection Act an essential legal basis for protecting data subjects.

Aditio et al. (2025) directly connected the principle of information disclosure with personal data protection in the information services of Religious Courts. Their study identified potential conflict between the duty to disclose information and the duty to safeguard private data, while emphasizing the importance of consequence testing and stronger interest-balancing assessments to ensure proportionate disclosure. Its focus, however, was judicial information services, whose documents, actors, and legal interests differ from those found in government procurement. Darmawan et al. (2026) examined procurement disclosure by comparing SPSE and the Electronic Catalog. Their findings indicate that SPSE provides relatively more complete information, whereas the Electronic Catalog and the INAPROC data dashboard still have limitations regarding information on mini-competitions, potentially narrowing the space for public oversight. These five studies provide an important foundation, but their analyses remain divided among procurement transparency, public participation, and personal data protection.

The theoretical framework of this article rests on legal harmonization theory and the principle of proportionality. Harmonization is required when two legal norms or interests point in different directions but must nevertheless operate within a single legal system. Safudin (2020) explains that legal antinomies should be addressed through harmonization in order to preserve legal unity, certainty, justice, proportionality, utility, and clarity. In the procurement context, information disclosure and personal data protection are treated as two interests that must be assessed according to their respective functions and the consequences of disclosure. The principle of proportionality is then used to determine whether restrictions on access to information are necessary, pursue a legitimate legal aim, and remain balanced in relation to their effects on both public rights and the rights of data subjects (Maulidina, 2024).

The academic concern arises because LKPP Head Decision Number 129 of 2025 provides a clearer classification of public and exempt information, yet the harmonization problem is not resolved merely by classifying documents. The Decision, for example, treats partnership agreement letters as exempt information by referring to Article 17 letters b and h of the Public Information Disclosure Act and the Personal Data Protection Act, while bidder identities in e-reverse auctions are also protected because they concern data relating to individual or entity participants. At the same time, certain information on work specifications, selection results, and contract summaries is designated as open after

completion of the work (LKPP, 2025a). This situation raises the question of how a document that is generally open should be treated when it contains personal data, trade secrets, signatures, personnel identities, or other information governed by a distinct protection regime. The issue is increasingly significant because digital publication allows information to be copied, stored, processed, and disseminated with considerable speed.

The five previous studies reveal a clear research gap. Studies on procurement transparency have primarily assessed the completeness of information and the capacity of electronic systems to provide public data, while studies on personal data protection have more often examined privacy safeguards in digital services or other sectors. Research directly connecting information disclosure and personal data has been conducted in the judicial context, but procurement information has distinctive characteristics because a single document may simultaneously involve public-budget interests, business competition, trade secrets, personal data, and the need for public oversight. More specifically, these five studies have not positioned LKPP Head Decision Number 129 of 2025 as the principal object for assessing the limits of procurement-information disclosure after the enactment of Law Number 27 of 2022. Darmawan et al. (2026), the most recent procurement study among them, focuses on comparing transparency in SPSE and the Electronic Catalog and does not center its analysis on the relationship between the document classifications under LKPP Head Decision Number 129 of 2025 and personal data protection obligations.

Against this gap, the novelty of this article lies in formulating a model for harmonizing procurement-information disclosure and personal data protection by placing LKPP Head Decision Number 129 of 2025 at the center of the analysis. Harmonization is directed toward three layers of assessment: the disclosure status of a document according to the procurement stage; identification of personal-data content or other legally protected interests; and consequence and proportionality testing before information is released to the public. This approach allows a document to fulfill its transparency function without requiring every data element to be disclosed uniformly. Measures such as identity redaction, data minimization, partial document disclosure, or access restrictions based on legitimate interests can operate as legal instruments for reconciling the two regulatory regimes (Budhijanto, 2024).

The urgency of this inquiry is reinforced by the continuing movement of government procurement toward an integrated digital ecosystem. LKPP has designated a personal data controller within its institutional environment through LKPP Head Decision Number 100 of 2025, indicating that data protection has become part of the institutional governance structure of procurement (LKPP, 2025b). This development requires public bodies to design consistent publication standards so that budget transparency does not result in excessive data disclosure, while data-protection arguments are not used broadly to conceal information that is genuinely necessary for public oversight.

Based on these issues, this article addresses two main questions: how are the limits of public information disclosure and personal data protection regulated in government goods/services procurement following LKPP Head Decision Number 129 of 2025, and what proportional harmonization model can reconcile the public's right to obtain procurement information with the obligation to protect personal data contained in procurement documents? In line with these questions, the article aims to analyze the legal construction of open and exempt information in government procurement and to formulate a harmonization framework for publication, redaction, restriction, and access to procurement information. The findings are expected to provide normative guidance for public bodies in maintaining procurement transparency, legal certainty, accountability in budget utilization, and balanced protection of personal-data rights.

METHOD

This study employs normative legal research using statutory and conceptual approaches. The statutory approach examines the relationship among rules on public information disclosure, personal data protection, and government goods/services procurement, particularly following the enactment of LKPP Head Decision Number 129 of 2025. The conceptual approach examines legal harmonization, transparency, accountability, the right to information, and personal data protection as the basis for assessing the limits of information disclosure in government procurement.

The legal materials consist of primary, secondary, and tertiary sources. Primary legal materials include Law Number 14 of 2008 on Public Information Disclosure, Law Number 27 of 2022 on Personal Data Protection, government procurement regulations, and LKPP Head Decision Number 129 of 2025 concerning the List of Public Information and the List of Exempt Information in Government Goods/Services Procurement. Secondary legal materials were obtained from scholarly journals, legal books, research findings, and academic publications addressing procurement transparency, information disclosure, and personal data protection. Tertiary legal materials were used to clarify terms, concepts, and legal constructions relevant to the object of study.

Legal materials were collected through literature review and examination of relevant legal documents. All collected materials were then analyzed qualitatively using prescriptive and interpretive analysis. The analysis involved inventorying legal norms, classifying open and exempt information, identifying potential conflicts between the right to information and the right to personal data protection, and testing the proportionality of restrictions on information access. The results were used to formulate a harmonization framework capable of preserving government-procurement transparency while providing adequate protection for personal data contained in procurement documents.

RESULTS AND DISCUSSION

Regulation of Public Information Disclosure in Government Goods/Services Procurement

Public information disclosure in government goods/services procurement is closely connected with state financial management because procurement is generally funded through the State Budget (APBN) or Regional Budgets (APBD). Every use of public funds entails accountability to society regarding planned needs, provider-selection processes, expenditure, and the outputs obtained. In this context, the principle of transparency requires sufficient, accurate, and accessible information so that the public has meaningful space to scrutinize governmental decisions. Transparency is also an element of governance that treats openness in decision-making processes as a basis for strengthening the accountability of public institutions (Karso, 2022).

Within the government procurement system, transparency has a more specific character because it relates to a sequence of activities from needs planning to the handover of completed work. Information at each stage carries a different oversight value. Procurement plans allow the public to understand the direction of budget expenditure, provider-selection information offers a picture of competition for government contracts, and contract-implementation information reveals the consistency among planning, budget value, and work outputs. Syafar et al. (2022) explain that procurement-information disclosure creates space for the public to monitor planning, selection, evaluation, contracts, and work results, thereby enabling the accountability of public bodies to be tested more openly.

This principle has become increasingly relevant as government procurement has moved into electronic systems. The Electronic Procurement System enables multiple procurement stages to be recorded digitally, allowing information on procurement packages, schedules, providers, prices, and selection results to be traced more systematically. Rahardjo et al. (2022) found that electronic procurement within LKPP has supported transparency and accountability because procurement processes refer to the General Procurement Plan published in the electronic system. Stored digital traces are also important for audit and oversight because procurement decisions leave administrative records that can be reviewed subsequently.

Regulatory developments have further strengthened the use of technology as a vehicle for disclosure. Presidential Regulation Number 46 of 2025 continues the regulation of electronic procurement by positioning SPSE and various supporting systems as part of government procurement administration. Digitalization creates opportunities for procurement information to reach a wider audience while accelerating the recording of processes that previously depended on conventional administrative documents. Zaenudin and Setyowati (2025) show that e-procurement can increase transparency when it is supported by clear regulation, organizational commitment, adequate human resources, and the use of digital media to expand public access to information.

The obligations of public bodies to provide procurement information are regulated more concretely in LKPP Head Decision Number 129 of 2025 concerning the List of Public Information and the List of Exempt Information in Government Goods/Services Procurement. The Decision covers the procurement process from the planning stage through handover of the completed work, while the

payment process falls outside its scope. At the planning stage, the General Procurement Plan is designated as information that must be announced through the General Procurement Plan Information System. Other public procurement information is, in principle, accessible after the work or procurement process has been declared complete (LKPP, 2025a).

This arrangement creates an important distinction in the timing of access. The General Procurement Plan is open from the planning stage because the public requires early information regarding projected government expenditure, while most selection-stage information is provided after completion of the work. The latter category includes work specifications, the Owner's Estimate within prescribed limits, information on contract type, provider requirements, selection-process requirements, work schedules and locations, providers' bid prices, clarification information, negotiated prices, winner information, and selection results. This policy demonstrates that procurement disclosure follows a stage-based approach so that public access remains available without disrupting ongoing competition (LKPP, 2025a).

Open information also includes information generated during contract implementation. LKPP Head Decision Number 129 of 2025 provides that a contract summary must at least contain the parties, contract value, scope of work, work location, funding source, implementation period, contract type, the reasons for contractual amendments where applicable, and information on work progress in terms of physical and financial achievement. Such information is opened after the work is completed. This structure is significant because public oversight of procurement extends to questions concerning the value of the contract, the scope of work to be delivered, and the extent to which actual performance corresponds with the government's contractual commitments (LKPP, 2025a).

Disclosure of this kind serves a preventive function against procurement irregularities. Procurement is an area vulnerable to bid-rigging, inflated work values, conflicts of interest, and various forms of budget misuse. Openness allows actors outside the procurement structure to compare plans, selection processes, prices, contracts, and actual implementation. Choiri and Hadi (2025) assess that regulatory reform through Presidential Regulation Number 46 of 2025 and the use of digital systems strengthen oversight and support accountability, although the quality of implementation continues to depend on infrastructure, human-resource capacity, and consistency of supervision.

At the implementation level, the existence of digital systems does not automatically guarantee the same quality of disclosure across all public bodies. The experience of the Magelang Regency Government shows that e-procurement is reasonably effective in expanding access to information, but challenges remain in human-resource capacity, infrastructure support, and technical issues in centralized systems (Zaenudin & Setyowati, 2025). This indicates that the duty to provide information requires orderly administrative governance. Commitment-Making Officials, selection working groups, procurement officials, and Information and Documentation Management Officers (PPID) need clearly defined responsibilities so that documents that should be available can be located, verified, and provided to information applicants in accordance with applicable rules.

Nevertheless, the principle of disclosure does not require every procurement document to be published without assessing the nature of the information it contains. LKPP Head Decision Number 129 of 2025 expressly distinguishes public information from exempt information. Documents that are confidential by nature, detailed HPS components containing calculations, survey results and unit prices, certain design drawings, and technical bids are subject to restrictions based on specified legal grounds and time periods. The underlying considerations concern the protection of business competition, trade secrets, intellectual property rights, security, and other legally protected interests (LKPP, 2025a). Under this framework, procurement transparency operates through information classification rather than uniform disclosure of all documents.

This change also addresses some of the problems identified in earlier literature. Syafar et al. (2022) noted uncertainty regarding the status of provider-evaluation data and differences among public bodies in determining which procurement information should be open or exempt. LKPP Head Decision Number 129 of 2025 provides a more structured list of information available to the public and information subject to lawful exemption. Legally, however, it is important to note that the Decision applies to public-information management within LKPP and may serve as a reference for ministries, agencies, and regional governments in establishing their own information lists according to their

respective authority. Consequently, nationwide consistency still requires follow-up by individual public bodies so that procurement-information classifications move toward aligned standards (LKPP, 2025a).

Accordingly, the regulation of public information disclosure in government procurement reflects a shift toward a more structured transparency mechanism. The public's right to information is fulfilled through publication of the General Procurement Plan, access to selection and contract information at prescribed times, and the provision of electronic information enabling oversight of budget utilization. At the same time, disclosure continues to take account of procurement stages and the characteristics of individual documents. This pattern positions openness as an instrument of public accountability that must be implemented carefully, measurably, and on a clear legal basis. Within the framework of good governance, the quality of transparency ultimately depends on the ability of public bodies to provide relevant, timely, and accurate information while maintaining justifiable access limitations (Karso, 2022).

Personal Data Protection in Government Procurement Documents and Systems

The digitalization of government goods/services procurement means that data are managed from the moment business actors register, submit qualification documents, participate in selection, sign contracts, and complete the work. Throughout this sequence, procurement systems may contain the names of company officers, identities of business representatives, telephone numbers, email addresses, signatures, personnel experience records, expert certificates, and certain financial information. Such data have administrative value for verifying the competence and legal standing of providers, yet they simultaneously create protection obligations when the information relates to identifiable individuals. Digital environments amplify risk because a document stored in a system can be replicated and disseminated on a much broader scale than a physical archive, meaning that data governance must incorporate security considerations from the point of collection (Sulistianingsih et al., 2023).

The first boundary that must be clarified concerns the meaning of personal data itself. Law Number 27 of 2022 defines personal data as data concerning an individual who is identified or identifiable, either directly or through a combination of other information. Consequently, information concerning a business entity as an entity, such as a company's name or legal form, does not automatically constitute personal data. Protection becomes relevant when corporate documents contain the identities of directors, owners, authorized representatives, experts, employees, or other individuals connected to the company. A full name is categorized as general personal data, while personal financial data constitute specific personal data because disclosure carries a higher level of risk for the individual concerned (Republic of Indonesia, 2022).

The next issue concerns the meaning of data processing. Article 16 of the Personal Data Protection Act includes acquisition, collection, processing, analysis, storage, correction, updating, display, announcement, transfer, dissemination, disclosure, deletion, and destruction as forms of personal-data processing. Under this construction, publishing procurement documents on government portals also constitutes personal-data processing when those documents contain information about individuals. A decision to disclose a document to the public must therefore be distinguished from a decision about which personal-data elements may properly be displayed. Data-governance principles require processing to be limited, specific, lawful, transparent, purpose-aligned, accurate, and accompanied by safeguards against unauthorized access and disclosure (Maharani & Prakoso, 2024).

In government procurement, personal-data processing does not always require consent as the sole legal basis. Article 20 of Law Number 27 of 2022 provides several lawful bases for processing, including valid consent, performance of contractual obligations, compliance with legal obligations, protection of vital interests, performance of tasks in the public interest or delivery of public services, exercise of authority under legislation, and other legitimate interests subject to a balance of rights. In government procurement, collecting the identities of company officers or provider personnel may therefore be based on legal obligations, contractual processes, or the exercise of governmental authority when such data are necessary to assess qualifications and perform contracts. The boundary lies in the relevance of the data to procurement purposes; the existence of a lawful basis does not authorize the use of data for purposes detached from the original reason for collection (Republic of Indonesia, 2022).

The principle of purpose limitation is particularly important because procurement documents frequently combine public information and personal information in a single file. The public, for example, has an interest in knowing which provider won a package, the value of the contract, and how

performance has progressed. Yet such oversight does not necessarily require publication of national identification numbers, personal bank-account numbers, signatures, private telephone numbers, residential addresses, or other elements that have no direct relationship to the objective of budget transparency. In these circumstances, partial masking or redaction is more proportionate than publishing the entire original document. Tjatur et al. (2024) emphasize that data management should follow the principles of purpose limitation, access control, security, and risk assessment for individuals before data are disseminated to other parties.

This approach receives a more concrete basis in LKPP Head Decision Number 129 of 2025. The Decision classifies partnership agreement letters as exempt information, referring among other grounds to the Personal Data Protection Act because disclosure may reveal private information while also affecting business-competition interests. The document is subject to a five-year exemption period following the records-retention schedule and, under certain conditions, may be provided to relevant parties. This normative choice demonstrates that the public interest in obtaining procurement information is limited when the content of a document enters the personal sphere or implicates other legally protected interests (LKPP, 2025a).

The same Decision gives special treatment to bidder identities in e-reverse auctions. Such information is classified as exempt on the ground that disclosure of identities may generate competitive pressure or conflict among participants, while non-disclosure is directed toward protecting data relating to individual or entity participants. From a data-protection perspective, an important conceptual distinction must be maintained: the identity of an individual falls under the Personal Data Protection Act, whereas information about a business entity may be protected under public-information law, competition law, trade-secret law, or procurement rules. This separation of legal grounds is important so that the label of personal data is not applied too broadly to conceal all information concerning providers that in fact has public-oversight value (LKPP, 2025a).

Protection responsibilities also attach to the design and operation of electronic procurement systems. Systems that store provider documents must regulate who is authorized to view data, what types of data may be downloaded, how long data are retained, how access is logged, and what procedures apply when a security incident occurs. Yusuf (2024) explains that electronic-system operators have a duty to maintain reliable and secure systems and to implement internal measures to prevent failures in data protection. Such governance is especially important in procurement because data move across multiple actors and stages, meaning that a weakness at one access point may expose information far beyond the original purpose for which it was collected.

LKPP's internal policy reflects the same direction through LKPP Head Decision Number 100 of 2025 on the Designation of a Personal Data Controller within LKPP. The Decision requires the controller to establish a lawful basis for processing, conduct processing in a limited and specific manner, record processing activities, ensure data accuracy, provide access to data subjects under specified conditions, conduct impact assessments for high-risk processing, maintain confidentiality, and prevent unauthorized access. The obligations also include terminating, deleting, or destroying data in accordance with the relevant purpose and retention period, as well as providing written notification when a personal-data protection failure occurs. Personal-data protection in procurement must therefore operate throughout the entire information life cycle, from receipt of the data until deletion or destruction in accordance with applicable requirements (LKPP, 2025b).

From a technological perspective, the concept of privacy by design is relevant to the development of procurement systems. This principle embeds privacy protection into system design from the outset, for example by limiting the data required in forms, classifying levels of sensitivity, assigning access rights according to user functions, redacting data before publication, and applying stronger safeguards to specific personal data. Sembiring et al. (2024) show that privacy-oriented design provides a preventive approach because protection considerations are introduced at the registration stage and when defining processing purposes, rather than only after risks emerge. In government procurement, this approach allows transparency to continue while reducing the likelihood that personal information will be disseminated merely because a system is designed to expose all document elements uniformly.

The balance ultimately depends on the relevance of information to the public interest. Data concerning provider names, bid prices, selection results, contract values, work progress, and other

information required to test accountability in the use of public funds have a strong basis for disclosure under public-information rules. By contrast, elements that reveal an individual's private life and contribute little to procurement oversight should be restricted, redacted, or exempted on a clear legal basis. The principle of balance under the Personal Data Protection Act requires reconciliation between individual rights over personal data and the broader interests of the state and society, meaning that both interests must be assessed according to the purpose, necessity, risk, and consequences of disclosure (Republic of Indonesia, 2022).

Implications of LKPP Head Decision Number 129 of 2025 for the Publication of Government Procurement Information

LKPP Head Decision Number 129 of 2025 introduces significant changes to procurement-information governance by providing a more detailed classification of information that is open and information that must be restricted. Before the Decision was issued, procurement-document information management within LKPP referred, among other instruments, to LKPP PPID Decision Number 3 of 2021 concerning the list of public information in procurement documents and LKPP PPID Decision Number 4 of 2021 concerning the classification of exempt information. Both decisions were expressly revoked when LKPP Head Decision Number 129 of 2025 took effect. This replacement reflects a policy shift from previously separate arrangements toward a single instrument that brings the list of public information and the list of exempt information together within one framework (LKPP, 2025a).

The scope of the Decision also establishes clearer administrative boundaries. Its information rules cover procurement from the planning stage through handover of completed work, while payment processes fall outside the scope of LKPP Head Decision Number 129 of 2025. This distinction is important because publication of procurement information often intersects with financial, payment, contract, and selection documents, each of which has different legal characteristics. The new policy provides a boundary enabling information managers to determine whether a document belongs to the procurement-information regime governed by the Decision or falls under another financial-information framework. Clarity regarding scope helps PPID and procurement units avoid expanding or restricting access on the basis of overly broad administrative interpretations (LKPP, 2025a).

A further implication concerns the timing of disclosure. The General Procurement Plan has a distinct status because it must be announced through the General Procurement Plan Information System from the planning stage. By contrast, other public procurement information is, in principle, accessible after the work or procurement process has been declared complete. This structure creates a stage-based disclosure model, under which the status of information is determined not only by document content but also by the time at which access is requested. A document that will ultimately be open need not necessarily be disclosed while competition is ongoing if disclosure at that stage could affect the selection process. Information managers must therefore identify the status of the procurement package before deciding whether to grant public access (LKPP, 2025a).

This time-based approach is particularly relevant to the digital character of procurement. Rakhman (2024) shows that procurement digitalization increases information accessibility and strengthens audit trails, although these benefits remain influenced by system governance, organizational readiness, and stakeholder participation. In the context of LKPP Head Decision Number 129 of 2025, electronic systems must therefore be capable of distinguishing data that may be displayed while a process is ongoing from information that may only be released after the activity has concluded. Stage-based access controls prevent digital disclosure from becoming premature disclosure that could disrupt competition, while preserving information trails for evaluation and oversight after procurement has ended.

At the selection stage, the Decision provides relatively broad access after completion of the work. Information categorized as open includes work specifications, contract type, provider requirements, selection-process requirements, work schedule and location, providers' bid prices, clarification information, negotiated prices, winner information, and selection results. The assignment of self-managed procurement teams and memoranda of understanding, where included in the listed categories, are likewise treated as public information. This structure gives the public a basis for reconstructing how a selection process unfolded after it has ended, from the nature of the government's needs to the final selection outcome. The availability of complete information is important because the

quality of public-information services is also determined by completeness, relevance, accuracy, timeliness, and the form in which information is presented to the public (Priyasta et al., 2024).

At the implementation stage, LKPP Head Decision Number 129 of 2025 adopts the contract-summary approach as one form of open information. The summary must at least contain the parties, contract value, scope and location of the work, funding source, implementation period, contract type, reasons for amendments where changes occur, and information on physical and financial progress. This design has important consequences for publication practice. The public interest in understanding the substance of budget utilization is satisfied through core contract information, while access to the entire contractual file is not automatically granted without assessing whether the file contains legally protected information. The summary model supports more targeted transparency because elements relevant to public accountability can be separated from sensitive information (LKPP, 2025a).

The most visible change, however, concerns the treatment of exempt information. LKPP Head Decision Number 129 of 2025 identifies several categories that are not generally open: procurement documents confidential by nature; detailed HPS components consisting of HPS calculations, survey results, and unit prices; design drawings; technical bids; responses to objections; responses to appeal objections; partnership agreement letters; and bidder identities in e-reverse auctions. These restrictions demonstrate that publication of procurement information must account for business competition, intellectual property rights, security, private information, data protection, and dispute-resolution interests. Information managers must therefore move away from an approach that assumes all procurement files have the same access status (LKPP, 2025a).

Detailed HPS components illustrate the rationale behind these restrictions. The Decision distinguishes procurement information that the public needs to know from the underlying HPS details, including calculations, survey results, and unit prices. According to the Decision's reasoning, disclosure of such data could allow business actors to obtain overly detailed price information, coordinate prices, or submit bids extremely close to the HPS, thereby reducing genuine competition. Confidentiality in this context is intended to preserve the quality of competition and reduce the risk of tender manipulation. Transparency is therefore not measured by the volume of documents uploaded, but by whether sufficient information is available for public oversight without undermining the competitive process that the procurement system is designed to protect (LKPP, 2025a).

A different rationale applies to design drawings and technical bids. Both forms of information may involve intellectual property, technical strategies, and the security of particular objects. Technical drawings of vital facilities, for example, may create security risks if detailed information can be accessed without restriction, while providers' technical bids may contain methods, designs, or business strategies that competitors could imitate. For technical bids, the exemption period is set at five years in line with the records-retention schedule, and access may be granted to relevant parties under specified conditions. This construction demonstrates that exemption functions as a limitation on who may access information and for how long, based on legally protected interests (LKPP, 2025a).

The same logic applies to responses to objections, responses to appeal objections, partnership agreement letters, and bidder identities in e-reverse auctions. Responses to objections and appeal objections are restricted to preserve the confidentiality of objection-resolution mechanisms and to prevent competitive pressure among procurement actors. Partnership agreement letters are restricted because they may contain both business secrets and personal data, making the Personal Data Protection Act one of the relevant normative bases. Bidder identities in e-reverse auctions are exempted to avoid pressure or conflict among participants. This configuration reflects a shift from disclosure based merely on document labels toward disclosure based on the risks created by releasing information (LKPP, 2025a).

The institutional implications are substantial for PPID and procurement units. Before publication, documents need to undergo coordination, verification, and validation so that released information corresponds with its classification, procurement stage, and applicable exemption rules. Priyasta et al. (2024) show that the quality of public-information services is linked to coordination and inter-unit verification before information is provided to the public. Ulumiyah and Gati (2024) likewise found that PPID portal management requires organizational capacity to adapt to regulatory developments and information needs, while limitations in personnel and knowledge of information

disclosure may remain obstacles. In procurement, the issue is even more technical because PPID must understand both public-information law and the stages and documentary characteristics of procurement.

LKPP Head Decision Number 129 of 2025 also has implications for ministries, agencies, and regional governments, but its normative position must be read carefully. The fourth dictum provides that the Decision applies to public-information management within LKPP and may be used as a reference by ministries, agencies, and regional governments when establishing lists of public and exempt information within their respective authority. The Decision therefore does not automatically replace the public-information and exempt-information lists established by each public body. In practical terms, every institution needs internal harmonization so that its procurement-document classifications move toward uniform standards. The importance of strengthening such governance is consistent with national evaluations of information disclosure, which treat information availability, institutional arrangements, services, and public-body compliance as important components of the quality of public information disclosure (Central Information Commission, 2024).

The Decision also preserves an adaptive mechanism for information not yet included in its lists. The sixth dictum allows changes based on the results of consequence testing for public-information requests that are not yet covered by the Decision. This provision is important because developments in procurement methods, electronic systems, and document types may generate new forms of information that were not anticipated when the regulation was drafted. Consequence testing operates as a mechanism for comparing the harm that may arise from disclosure with the interests protected by withholding the information. This model prevents the exemption list from becoming a rigid and permanent administrative justification for rejecting every information request (LKPP, 2025a).

Overall, LKPP Head Decision Number 129 of 2025 shifts the orientation of procurement-information publication toward governance that is classified, staged, and risk-based. The General Procurement Plan remains public from the planning stage, whereas most selection and implementation information becomes accessible after the process or work is complete. Information that risks damaging competition, revealing business secrets, exposing personal data, compromising security, or disclosing technical strategies is placed under an exemption regime for specified periods. This pattern is consistent with the development of procurement digitalization, which expands access and strengthens audit trails while simultaneously requiring control over information disseminated through electronic systems (Rakhman, 2024). The Decision's principal implication therefore lies in changing how public bodies determine what should be disclosed, when disclosure should occur, which parts should be restricted, who may obtain access, and what legal basis supports each restriction.

Harmonizing Transparency and Personal Data Protection in Government Procurement Following LKPP Head Decision Number 129 of 2025

Transparency and personal data protection arise from two legal interests that are both legitimate in public administration. Transparency gives the public access to information on budget utilization, provider-selection processes, contract values, and government work outputs. At the same time, every individual whose data enter the procurement system has an interest in security, confidentiality, and the use of data in accordance with the purposes for which they were collected. Tension emerges when a single document contains both types of interest, for example a contract that contains a procurement value as public information alongside the names, signatures, addresses, contact numbers, or other personal identifiers of the parties involved. Oktavianti et al. (2026) show that conflict between the right to information and the right to privacy requires proportionality and information classification so that public accountability can continue without producing excessive disclosure of personal data.

This tension is particularly pronounced in government procurement because procurement processes bring public and private interests together within a single digital ecosystem. Providers submit various forms of data to demonstrate legal standing, capacity, experience, expert personnel, and administrative sufficiency, while the government is obliged to provide certain information to the public as accountability for the use of public funds. Data integration in government systems can improve service efficiency, but combining and exchanging information across units also increases the risk that data will be used beyond their original purpose if access and security controls are inadequate. Rahmawati et al. (2025) emphasize the need for consistent governance, supervision, and information-security mechanisms when personal data are processed through interconnected government systems.

LKPP Head Decision Number 129 of 2025 provides an initial framework for harmonization by explicitly distinguishing open procurement information from exempt information. The Decision affirms that procurement disclosure must guarantee the public's right to information while continuing to protect confidential information under applicable legislation. The General Procurement Plan is disclosed from the planning stage through SiRUP, while other public information is, in principle, accessible after the work or procurement process has been completed. This construction demonstrates that harmonization does not require an absolute choice between openness and confidentiality; rather, it is achieved through regulation of the substance of information, the timing of disclosure, and the purposes for which information is used (LKPP, 2025a).

The first point of conflict appears in documents that are substantively necessary for testing accountability but also contain personal-data elements. A contract summary, for example, is designated as public information and must at least identify the parties, contract value, scope of work, location, source of funds, implementation period, contract type, reasons for contractual amendments, and physical and financial achievement. These elements matter to the public because they can be used to assess the correspondence between government expenditure and work results. Yet disclosure of a contract summary does not automatically justify publication of national identification numbers, personal bank-account numbers, residential addresses, private telephone numbers, copies of identity documents, or other data unrelated to the purpose of budget oversight. The contract-summary model under the LKPP Decision therefore points toward transparency centered on the substance of accountability rather than uniform disclosure of entire documents (LKPP, 2025a).

This legal boundary can be formulated through the principle of data minimization. Once the purpose of disclosure is satisfied through the business entity's name, contract value, scope of work, source of funding, and implementation results, adding irrelevant personal data increases risks to data subjects without producing a proportionate oversight benefit. In digital government, data processing must have a clear purpose and be accompanied by access controls, security measures, and controller accountability for each use of information. Rahmawati et al. (2025) show that integrated government data require clear access restrictions and security mechanisms because data connected across systems carry a greater risk of dissemination than data managed within limited environments.

A second point of conflict concerns information directly related to competition among business actors. Transparency is necessary to ensure a fair selection process, but disclosure that is too early or too detailed may expose bidding strategies and distort competition. LKPP Head Decision Number 129 of 2025 therefore distinguishes the HPS, which may be disclosed after completion of the work, from detailed HPS components such as calculations, survey results, and unit prices, which are classified as exempt. The reasoning is concrete: price data may be used to coordinate prices, generate bids extremely close to the HPS, or reduce healthy competition. This exemption demonstrates that transparency is not measured by the volume of data published, but by the sufficiency of information for oversight without creating greater harm to the competitive system (LKPP, 2025a).

A similar conflict appears in partnership agreement letters. LKPP Head Decision Number 129 of 2025 specifically classifies them as exempt information on the basis of Article 17 letters b and h of the Public Information Disclosure Act and Law Number 27 of 2022 on Personal Data Protection. Disclosure is considered capable of undermining intellectual-property protection, business competition, and personal confidentiality. The Decision imposes a five-year exemption period in accordance with the records-retention schedule, while allowing access for relevant parties. This provision demonstrates a direct intersection between disclosure and data-protection regimes: a justification for withholding information must be linked to a specific risk, be time-limited, and not be used to conceal other procurement information that continues to carry a public interest (LKPP, 2025a).

Bidder identities in e-reverse auctions likewise demonstrate the need for a more precise distinction between business-entity data and data concerning natural persons. The LKPP Decision classifies bidder identities in that mechanism as exempt for five years because disclosure may generate competitive pressure or conflict among participants. However, the phrase concerning protection of data relating to individual or entity participants must be applied carefully. The Personal Data Protection Act specifically protects data concerning natural persons, whereas the confidentiality of business-entity information may be protected under competition law, trade-secret law, contractual rules, or procurement

regulation. Separating these legal grounds is necessary so that the concept of personal data does not become a general basis for concealing every piece of information concerning companies participating in tenders (LKPP, 2025a).

Harmonization at the normative level must also take account of the position of LKPP Head Decisions within the legal system. LKPP Head Decision Number 129 of 2025 provides an operational classification of procurement information, while the fundamental limits of rights and obligations continue to derive from the Public Information Disclosure Act and the Personal Data Protection Act. The list of exempt information should therefore not operate as an automatic reason to reject every request. Information Commission Regulation Number 1 of 2021 emphasizes that exempt information must be construed strictly and narrowly and may consist of an entire document or only particular information contained within it. Before information is declared exempt, the PPID is required to conduct a consequence test (Information Commission of the Republic of Indonesia, 2021).

Consequence testing is a central instrument for reconciling transparency and data protection. Information Commission Regulation Number 1 of 2021 requires the PPID to identify clearly the information proposed for exemption, determine its legal basis, and consider the consequences of disclosure based on propriety, morality, the public interest, and other applicable legal provisions. Testing may be conducted before a request is submitted, when a request is made, or during the resolution of an information dispute. Under this mechanism, the fact that a document contains personal data is not, by itself, sufficient to justify withholding the entire document when personal elements can be separated from parts that carry public-accountability value (Information Commission of the Republic of Indonesia, 2021).

Partial access is the logical consequence of this principle. Procurement documents may still be disclosed after certain information has been blacked out or redacted when protected portions can be separated from open information. Information Commission Regulation Number 1 of 2021 even requires written notice to an applicant to explain any blacking out or redaction that has been applied. In procurement practice, this mechanism may involve disclosing contract values, business-entity names, the object of the work, funding sources, and work progress while masking identification numbers, bank-account numbers, certain electronic signatures, personal addresses, or other sensitive information that is unnecessary for oversight. This approach preserves disclosure without sacrificing an entire document merely because it contains one or more protected elements (Information Commission of the Republic of Indonesia, 2021).

The need for proportionate restrictions is not merely theoretical. The 2024 Public Information Disclosure Index recorded a national score of 75.74 for the indicator measuring proportionality of disclosure restrictions, down from 76.06 in 2023 and still within the medium category. The report also found that public bodies continue to restrict information and that refusals are not always accompanied by adequate reasons; goods/services procurement is among the sectors identified as facing problems concerning information restrictions. These findings reveal two simultaneous risks: public bodies may disclose too much and expose data that should be protected, or they may become excessively restrictive by using exemptions to obstruct public oversight (Central Information Commission, 2024).

Experience with information disputes also demonstrates the importance of separating open parts of documents from portions that have lawful grounds for exemption. In 2024, the Central Information Commission handled a dispute between the Association for State Financial Monitoring and the Ministry of Communication and Informatics concerning government procurement contract documents. The dispute ended through mediation, with the respondent agreeing to provide the requested information in digital form. Cases of this kind show that procurement contracts carry significant public-oversight value and that withholding information requires a measurable legal justification. At the same time, disclosure of a contract may still be accompanied by redaction of particular portions when the document contains information entitled to special protection (Central Information Commission, 2024).

Theoretically, an appropriate harmonization model should not be directed toward the dominance of one legal regime over another. Safudin (2021) describes harmonization as an effort to create coherence where multiple norms generate tension in application, enabling the relationship among rules to operate consistently and in balance. In procurement, the Public Information Disclosure Act directs administrators toward accountability through disclosure, while the Personal Data Protection Act regulates the limits of using data concerning natural persons. Both can operate within the same document

through classification, separation of information, purpose limitation, data redaction, time-based access rules, and consequence testing. This approach is more appropriate than using one legal regime to eliminate interests protected by the other.

Harmonization thinking has also developed in digital data governance. Vanessa et al. (2026) show that harmonization of data protection can be pursued through interoperability, meaning that protection standards are aligned without eliminating the function and character of each legal system. This idea is relevant to procurement because transparency standards and data-protection standards need to operate interoperably. Procurement systems may continue to provide information required for public audit, but their publication function should be distinguished from internal-storage functions. Complete data may remain available to authorized officials for verification, audit, supervision, or law-enforcement purposes, while public-facing displays contain only data elements directly related to transparency interests.

On this basis, proportionate legal limits for procurement publication can be formulated through three interconnected stages. First, a public body assesses the public interest in the information, particularly its relationship to budgets, competition, provider selection, contracts, and work results. Second, the public body identifies disclosure risks, including personal data, trade secrets, intellectual property rights, security, and possible disruption of competition. Third, the least restrictive measure capable of achieving a balance is selected, ranging from full publication, publication after completion of the process, redaction of particular portions, special access for parties with a legal interest, to exemption where the consequences of disclosure would be demonstrably more harmful. This mechanism is consistent with the principle that information exemptions must be strict, limited, legally grounded, and supported by consequence analysis (Central Information Commission, 2024).

Accordingly, LKPP Head Decision Number 129 of 2025 provides a more concrete basis for connecting procurement disclosure with the protection of sensitive information, but the effectiveness of harmonization still depends on how its classifications are implemented. Transparency should not result in publication of every item of data stored in a system, while personal data protection should not be used to conceal contract values, the identity of winning business entities, funding sources, scopes of work, or implementation results that directly relate to public accountability. A proportionate boundary lies in relevance, purpose, necessity, risk, timing of disclosure, and the possibility of separating protected information from open information. Through this approach, procurement governance can preserve meaningful space for public oversight while protecting the rights of data subjects in a digital-government ecosystem.

CONCLUSION

Based on the research questions, the regulation of public information disclosure in government goods/services procurement following LKPP Head Decision Number 129 of 2025 reflects a more directed model of information governance through the distinction between open and exempt information. The General Procurement Plan remains publicly announced from the planning stage, while other information, including selection results, winner information, contract summaries, contract values, funding sources, scopes of work, and physical and financial progress, becomes accessible after the procurement process or work has been completed. At the same time, detailed HPS components, technical bids, partnership agreement letters, responses to objections, responses to appeal objections, certain design drawings, and bidder identities in e-reverse auctions are classified as exempt because they implicate business competition, trade secrets, intellectual property, security, and personal data protection. The framework demonstrates that procurement disclosure continues to be maintained, but publication must take into account the nature of the document, the stage of procurement, and the consequences that may arise from disclosure.

Harmonization between transparency and personal data protection must be implemented through proportionate legal boundaries. Information directly related to the use of public funds, the identity of the winning business entity, contract values, the object of the work, funding sources, selection results, and implementation achievements should remain available to safeguard accountability. By contrast, elements such as national identification numbers, personal bank-account numbers, residential addresses, private contact numbers, signatures, personal financial data, and other information irrelevant

to oversight should be redacted or restricted. The most appropriate model is needs- and risk-based publication through consequence testing, partial data redaction, time-based disclosure, and restricted access for parties with a legitimate legal interest. Under this model, LKPP Head Decision Number 129 of 2025 can function as an operational foundation for balancing the public's right to procurement information with individuals' rights to personal data protection.

RESEARCH LIMITATIONS

This study remains limited by its normative legal approach, which relies on legislation, institutional decisions, books, and scholarly articles and therefore does not directly portray the implementation of LKPP Head Decision Number 129 of 2025 across ministries, agencies, and regional governments. In addition, the Decision is relatively recent, so there are not yet many information-dispute decisions, institutional evaluations, or empirical datasets capable of demonstrating the consistency with which information classifications are applied across different procurement systems. Future research should combine normative and empirical approaches through interviews with PPID officials, Government Procurement Units (UKPBJ), providers, and information applicants, while comparing publication practices across several institutions in order to assess effectiveness, implementation barriers, and compliance with disclosure and personal data protection principles more measurably.

REFERENCES

Aditio, R., Epandi, Pratiga, N., Al Ayyubiy, M. S., Wati, E. W., Mutiara, Khoiriah, M. S., & Ahmad. (2025). Harmonisasi asas keterbukaan informasi dan perlindungan data pribadi dalam layanan informasi di Pengadilan Agama [Harmonization of information disclosure and personal data protection principles in Religious Court information services]. Islamitsch Familierecht Journal, 6(2), 138-154. https://doi.org/10.32923/wv4xa352

Baihaki, & Rachman, A. (2022). Modul pelatihan kompetensi pengadaan barang/jasa pemerintah level 1: Pengantar pengadaan barang/jasa pemerintah [Level 1 government procurement competency training module: Introduction to government goods/services procurement]. Pusat Pendidikan dan Pelatihan Pengadaan Barang/Jasa, LKPP.

Budhijanto, D. (2024). Hukum pelindungan data pribadi & data nasional [Law on personal data protection and national data]. Logoz Publishing.

Choiri, I., & Hadi, H. (2025). Analisis pengaruh regulasi terbaru Perpres Nomor 46 Tahun 2025 dan Sistem E-Katalog V.06 terhadap nilai efektif, efisien, akuntabilitas dan transparansi pada pengadaan barang/jasa pemerintah [Analysis of the effect of Presidential Regulation Number 46 of 2025 and E-Catalog V.06 on effectiveness, efficiency, accountability, and transparency in government procurement]. Jurnal Pengadaan Barang dan Jasa, 4(2), 52-69. https://doi.org/10.55961/jpbj.v4i2.71

Darmawan, S. A., Adzkasyah, M., Fandil, A., & Laksana, B. P. (2026). Keterbukaan informasi publik dalam pengadaan barang/jasa pemerintah: Analisis komparatif transparansi SPSE dan Katalog Elektronik [Public information disclosure in government procurement: A comparative analysis of SPSE and Electronic Catalog transparency]. Jurnal Pengadaan Indonesia, 5(1). https://doi.org/10.59034/jpi.v5i1.103

Karso, A. J. (2022). Buku ajar good governance [Good governance textbook]. Samudra Biru.

Komisi Informasi Pusat Republik Indonesia. (2024). Indeks keterbukaan informasi publik 2024 [2024 Public Information Disclosure Index]. Komisi Informasi Pusat Republik Indonesia.

Komisi Informasi Republik Indonesia. (2021). Peraturan Komisi Informasi Republik Indonesia Nomor 1 Tahun 2021 tentang Standar Layanan Informasi Publik [Information Commission Regulation Number 1 of 2021 on Public Information Service Standards].

Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah. (2025a). Keputusan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 129 Tahun 2025 tentang Daftar Informasi Publik dan Daftar Informasi yang Dikecualikan pada Pengadaan Barang/Jasa Pemerintah [LKPP Head Decision Number 129 of 2025 on the List of Public Information and the List of Exempt Information in Government Goods/Services Procurement]. LKPP.

Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah. (2025b). Keputusan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 100 Tahun 2025 tentang Penetapan

Pengendali Data Pribadi di Lingkungan Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah [LKPP Head Decision Number 100 of 2025 on the Designation of a Personal Data Controller within LKPP]. LKPP.

Maharani, R., & Prakoso, A. L. (2024). Perlindungan data pribadi konsumen oleh penyelenggara sistem elektronik dalam transaksi digital [Consumer personal data protection by electronic-system operators in digital transactions]. Jurnal USM Law Review, 7(1), 333-347. https://doi.org/10.26623/julr.v7i1.8705

Manurung, E. A. P., & Thalib, E. F. (2023). Tinjauan yuridis perlindungan data pribadi berdasarkan UU Nomor 27 Tahun 2022 [Juridical review of personal data protection under Law Number 27 of 2022]. Jurnal Hukum Saraswati, 4(2), 139-148.

Maulidina, E. I. (2024). Urgensi uji kebutuhan dan proporsionalitas dalam pengecualian hak-hak subjek data pribadi di Indonesia [The urgency of necessity and proportionality tests in exceptions to personal-data subject rights in Indonesia]. Jurnal Analisis Hukum, 7(2), 143-159. https://doi.org/10.38043/jah.v7i2.5464

Oktavianti, R. T., Nur, I. T., & Erwinta, P. (2026). Keseimbangan hak atas informasi dan privasi dalam pengelolaan data pribadi pejabat publik [Balancing the right to information and privacy in managing the personal data of public officials]. PESHUM: Jurnal Pendidikan, Sosial dan Humaniora, 5(4), 10243-10256. https://doi.org/10.56799/peshum.v5i4.16797

Priliasari, E. (2023). Perlindungan data pribadi konsumen dalam transaksi e-commerce menurut peraturan perundang-undangan di Indonesia [Protection of consumers' personal data in e-commerce transactions under Indonesian legislation]. Jurnal RechtsVinding: Media Pembinaan Hukum Nasional, 12(2), 261-279.

Priyasta, M. R. Y. E., Ramdhani, M., & Ema. (2024). Peranan PPID dalam pelayanan informasi publik di Dinas Kominfo Karawang [The role of PPID in public-information services at the Karawang Communication and Informatics Office]. Jurnal Pendidikan Tambusai, 8(2), 24028-24037.

Rahardjo, S., Bijaksana, G., Larasati, K., Chamsudi, D. H. M., Sitorus, P. P., & Kania, D. D. (2022). Analisis akuntabilitas dan transparansi sistem elektronik pengadaan barang dan jasa pemerintah di LKPP [Analysis of accountability and transparency in LKPP's electronic government procurement system]. Jurnal Sistem Transportasi & Logistik, 2(1), 82-90. https://doi.org/10.54324/jstl.v2i1.1262

Rahmawati, D. S., Rosadi, S. D., & Cahyadini, A. (2025). Implementasi pelindungan data pribadi berupa Nomor Induk Kependudukan (NIK) dan Nomor Pokok Wajib Pajak (NPWP) pada Sistem Pemerintahan Berbasis Elektronik menurut Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Implementation of personal data protection for national identification and taxpayer identification numbers in electronic-based government systems under Law Number 27 of 2022]. Media Hukum Indonesia, 3(2), 739-749. https://doi.org/10.5281/zenodo.15857274

Rakhman, A. A. (2024). Tinjauan sistematik tentang pengaruh digitalisasi pengadaan terhadap efisiensi dan transparansi di sektor publik Indonesia [A systematic review of the effects of procurement digitalization on efficiency and transparency in Indonesia's public sector]. Jurnal Pengadaan Indonesia, 3(2), 78-90. https://doi.org/10.59034/jpi.v3i2.53

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Law Number 27 of 2022 on Personal Data Protection].

Resminingayu, D. H. (2022). Keterlibatan publik dalam komitmen transparansi pengadaan barang dan jasa di Indonesia melalui platform Global Open Government Partnership [Public involvement in Indonesia's procurement-transparency commitments through the Global Open Government Partnership platform]. Jurnal Keterbukaan Informasi Publik, 2(4), 5-10.

Rifaid, & Zulkarnain. (2021). Transparansi pengadaan barang dan jasa pemerintah secara elektronik (e-procurement) di Nusa Tenggara Barat 2017-2020 [Transparency in electronic government procurement (e-procurement) in West Nusa Tenggara, 2017-2020]. Indonesian Governance Journal, 4(1).

Safudin, E. (2020). Harmonisasi hukum dalam antinomi hukum: Analisis terhadap penerapan Pasal 20 ayat (2) huruf b Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman [Legal harmonization in legal antinomies: Analysis of the application of Article

20(2)(b) of Law Number 48 of 2009 on Judicial Power]. Al-Syakhsiyyah: Journal of Law and Family Studies, 2(2), 201-229. https://doi.org/10.21154/syakhsiyyah.v2i2.2592

Safudin, E. (2021). Harmonisasi hukum dalam antinomi hukum: Telaah kritis atas penerapannya oleh Mahkamah Agung [Legal harmonization in legal antinomies: A critical review of its application by the Supreme Court]. Q Media.

Sembiring, P. E., Ramli, A. M., & Rafianti, L. (2024). Implementasi desain privasi sebagai pelindungan privasi atas data biometrik [Implementation of privacy by design for protecting biometric-data privacy]. Veritas et Justitia, 10(1), 127-152. https://doi.org/10.25123/vej.v10i1.7622

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse: Telaah yuridis Undang-Undang Perlindungan Data Pribadi [Personal data protection governance in the metaverse era: A juridical review of the Personal Data Protection Act]. Masalah-Masalah Hukum, 52(1), 97-106. https://doi.org/10.14710/mmh.52.1.2023.97-106

Syafar, I., Husen, L. O., & Razak, A. (2022). Urgensi keterbukaan informasi publik data evaluasi penyedia pengadaan barang/jasa pemerintah [The urgency of public disclosure of provider-evaluation data in government procurement]. Journal of Lex Generalis, 3(3), 418-437.

Tjatur, H., Irene, D., Wardana, B., & Riyanto, G. D. (2024). Modul pelindungan data pribadi dalam jurnalisme dan media [Personal data protection module for journalism and media]. Aliansi Jurnalis Independen.

Ulumiyah, P. R., & Gati, R. A. (2024). Meningkatkan keterbukaan publik: Strategi humas pemerintahan dalam pelayanan informasi publik pada portal website PPID Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi [Enhancing public openness: Government public-relations strategies in public-information services through the PPID portal of the Ministry of Administrative and Bureaucratic Reform]. Jurnal Pembangunan dan Administrasi Publik, 6(1).

Vanessa, C., Tan, D., & Agustianto, A. (2026). Harmonisasi hukum pelindungan data pribadi di Indonesia dan Singapura dalam kerangka Asia-Pacific Economic Cooperation Privacy Framework [Harmonization of personal data protection law in Indonesia and Singapore within the Asia-Pacific Economic Cooperation Privacy Framework]. Nomos: Jurnal Penelitian Ilmu Hukum, 6(1), 84-101. https://doi.org/10.56393/nomos.v6i1.4578

Yusuf, P. A. (2024). Tanggung jawab keamanan data digital oleh penyelenggara sistem elektronik [Responsibility for digital-data security by electronic-system operators]. Lex Privatum, 13(5).

Zaenudin, A., & Setyowati, Y. (2025). Implementasi kebijakan e-procurement dalam mewujudkan transparansi pengadaan barang/jasa pada Pemerintah Kabupaten Magelang [Implementation of e-procurement policy to realize transparency in goods/services procurement in the Magelang Regency Government]. Journal of Indonesian Rural and Regional Government, 9(1), 294-309. https://doi.org/10.47431/jirreg.v9i1.709