JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i5

Cross-Border Personal Data Transfer Requirements under Law Number 27 of 2022 on Personal Data Protection: Normative Clarity and Legal Protection

Diana Puji Ratna Kusuma Fitri[1*], Hananto Widodo[2], Budi Hermono[3].
[1]State University of Surabaya, Surabaya, Indonesia, email: 24131585013@mhs.unesa.ac.id
[2]State University of Surabaya, Surabaya, Indonesia, email: hanantowidodo@unesa.ac.id
[3]State University of Surabaya, Surabaya, Indonesia, email: budihermono@unesa.ac.id

[*]Corresponding Author: 24131585013@mhs.unesa.ac.id

Abstract: This article examines the normative construction of Article 56 of Law Number 27 of 2022 on Personal Data Protection, which regulates the requirements for cross-border personal data transfers. The study is motivated by the increasing transfer of personal data within the digital ecosystem, which may weaken the protection of data subjects' rights if it is not supported by clear legal norms. This study aims to analyze the normative construction of Article 56 and the implications of its normative ambiguity for legal certainty and the legal protection of data subjects. This study employs a normative legal research method using statutory, conceptual, and limited comparative approaches. The findings show that Article 56 establishes three requirements for cross-border personal data transfers, namely an equivalent or higher level of protection, adequate and binding protection, and the consent of the data subject as a last resort. However, this provision does not yet provide clear normative parameters regarding the standard of equivalent protection, the form of adequate and binding safeguards, or the limits on the use of consent. Therefore, Article 56 needs to be clarified in order to provide legal certainty and ensure the protection of data subjects' rights in cross-border personal data transfers.

Keyword: Cross-Border Personal Data Transfer, Article 56 Personal Data Protection, Legal Certainty, Legal Protection

INTRODUCTION

The development of the digital economy, cloud computing, global platform services, and integrated electronic transactions has made cross-border personal data transfers an increasingly common practice. Such data flows support efficiency, innovation, and global connectivity. At the same time, however, they raise legal concerns when personal data is transferred to jurisdictions that provide different or lower standards of protection than Indonesia (Ayiliani & Farida, 2024). This situation places data subjects in a vulnerable position because the legal protection applicable in Indonesia does not always guarantee the continuity of data subjects' rights once the data is located outside the national jurisdiction (Nafisa et al., 2025).

Article 56 of Law Number 27 of 2022 on Personal Data Protection (hereinafter referred to as the Personal Data Protection Law) serves as the primary legal basis for the requirements governing the transfer of personal data outside the territory of Indonesia. This article provides three requirements, namely that the recipient country must provide an equivalent or higher level of protection, that there must be adequate and binding personal data protection, and that the consent of the data subject may be used as a last resort. The elucidation of the law states that the provision of Article 56 is "sufficiently clear." However, normative ambiguity remains, particularly because the provision does not establish clear normative measures regarding the meaning of an equivalent level of protection, the form of adequate and binding protection, or the limits on the use of consent. This ambiguity is important to examine because it may create legal uncertainty and weaken the protection of data subjects' rights in cross-border personal data transfers (Maramis et al., 2024; Tjatur et al., 2024; Tomasoa, 2024).

Viewed from its normative construction, Article 56 of the Personal Data Protection Law does not merely regulate the administrative procedure for transferring data abroad, but also reflects the presence of the state in limiting the risk of data misuse before the transfer is carried out. Such state involvement is important because, in cross-jurisdictional transfers, the consent of the data subject is not always sufficient to ensure effective protection. In practice, data subjects are often in an unequal position, do not fully understand the legal consequences of the transfer, and lack the ability to assess whether the legal regime of the recipient country genuinely provides an equivalent level of protection. Therefore, the legal screening mechanism under Article 56 of the Personal Data Protection Law should be understood as a form of preventive legal protection, namely a norm that operates before harm occurs, rather than merely as a formal basis of legitimacy for personal data controllers to transfer data to another jurisdiction. The requirements under Article 56 of the Personal Data Protection Law are important because data transfers cannot be justified solely by business needs or technical efficiency; rather, they must be assessed through normative standards that ensure the continuity of the protection of data subjects' rights.

The Personal Data Protection Law adopts a concept similar to the mechanisms of adequacy decisions and appropriate safeguards under the GDPR. According to Gregory (2022), restrictions on cross-border personal data transfers under the GDPR aim to ensure that the level of protection for data subjects guaranteed by the GDPR is not diminished as a result of the transfer of data to another country. Therefore, every personal data transfer must comply with certain legal mechanisms so that the continuity of the protection of data subjects' rights remains guaranteed. The success of cross-border personal data transfer mechanisms depends on the clarity of the norms governing protection standards and the legal instruments used.

This study employs the theories of legal certainty and legal protection as its analytical framework. The theory of legal certainty, as a fundamental value in the legal system according to Gustav Radbruch (Manullang, 2017), is used to assess whether the formulation of Article 56 of the Personal Data Protection Law provides clear, consistent, and predictable parameters for personal data controllers, data subjects, and supervisory authorities. Meanwhile, the theory of legal protection is used to assess the capacity of the norm to provide preventive and repressive protection for the rights of data subjects (Hadjon, 1987). In the context of cross-border data transfers, legal protection cannot stop at formal authorization or consent; it must also ensure the continuity of rights, the accountability of personal data controllers, and the availability of legal remedies in the event of a violation (Jiménez-Gómez & Sofía, 2021).

Several previous studies have discussed personal data protection under the Personal Data Protection Law, including issues related to the need for implementing regulations, supervisory institutions, risks of data breaches, and comparisons with international data protection regimes. However, studies that specifically examine the normative construction of Article 56 of the Personal Data Protection Law as the legal basis for the requirements of cross-border personal

data transfers remain limited. Normative clarity at the statutory level is an important prerequisite for the formulation of implementing regulations, the compliance of personal data controllers, and the enforcement of data subjects' rights. In this context, the phrases concerning an equivalent level of protection, adequate and binding protection, and consent as a last resort need to be analyzed normatively so that they do not give rise to multiple interpretations or uncertain compliance burdens (Charles & Oktawijaya, 2026; Jurcys et al., 2022).

Based on the foregoing discussion, the problem addressed in this study concerns the normative issues surrounding the clarity of cross-border data transfer requirements in Indonesia. This study analyzes the normative construction of Article 56 of the Personal Data Protection Law and the implications of its normative ambiguity. The purpose of this study is to examine the norms governing cross-border data transfers in relation to legal certainty and the protection of data subjects' rights. The novelty of this study lies in its positioning of Article 56 of the Personal Data Protection Law not merely as an administrative provision on data transfers, but as a norm that determines the continuity of legal protection after personal data leaves Indonesia's jurisdiction.

METHOD

This study constitutes normative legal research that examines the ambiguity in the regulation of cross-border personal data transfers under Article 56 of the Personal Data Protection Law. The study applies deductive and inductive reasoning in a complementary manner. Deductive reasoning is used to apply general legal rules, including constitutional norms, legal principles, statutory regulations, the theory of legal certainty, and the theory of legal protection, to the issue of ambiguity in the requirements for transferring personal data abroad. Inductive reasoning is used to identify the concepts, principles, and legal consequences of the existing regulation in order to formulate a more appropriate regulatory direction within the national legal system.

The approaches employed in this study include the statutory approach, the conceptual approach, and a limited comparative approach. The statutory approach is used to examine positive law governing personal data protection and cross-border personal data transfers, including the ratio legis, philosophical foundations, and normative consistency within the national legal system. The conceptual approach is used to formulate the meaning of an equivalent level of protection, adequate and binding protection, and the consent of the data subject as a last resort. The comparative approach is used in a limited manner by comparing the concept of cross-border data transfers under the Personal Data Protection Law with the principles of adequacy and appropriate safeguards under the The General Data Protection Regulation (GDPR).

The legal materials used in this study consist of primary legal materials, namely the 1945 Constitution of the Republic of Indonesia and the Personal Data Protection Law; secondary legal materials, including books, journal articles, research findings, legal doctrines, and legal literature; and supporting legal materials relevant to personal data protection and international law. Legal materials are collected through the study of statutory documents and library research. The analysis of legal materials is conducted prescriptively and evaluatively by examining the normative construction and the implications of normative ambiguity in order to assess the adequacy of Article 56 of the Personal Data Protection Law in providing legal certainty and legal protection for data subjects in cross-border data transfers.

RESULTS AND DISCUSSION

The Normative Construction of Article 56 of the Personal Data Protection Law on the Requirements for Cross-Border Data Transfers

Cross-border personal data transfers can no longer be viewed as a supplementary activity in digital economic relations, but rather as an inherent part of cloud computing services, trade through electronic systems, digital identity interoperability, and the integration of global platforms. In such practices, personal data does not only include basic identity information, but may also cover consumer preferences, transaction behavior, location data, population data, and financial data with a high degree of sensitivity. Therefore, the transfer of data to another jurisdiction always entails legal risks, particularly when the recipient country has different protection standards, weak supervisory mechanisms, or patterns of state and corporate access that are not aligned with the principles of personal data protection.

In the context of the development of the global digital economy, the transfer of personal data outside national jurisdiction is not merely a technical movement between systems, but a legal event that directly affects the continuity of the protection of data subjects' rights. Personal data has become part of the infrastructure of the digital economy that supports cloud computing services, electronic commerce, digital identity, and cross-platform service management. Therefore, the regulation of data transfers must be able to respond not only to the needs of efficiency and innovation, but also to the risks of data misuse, changes in legal regimes, and the reduced ability of the state to guarantee the rights of its citizens once the data is located outside Indonesia's jurisdiction.

Article 56 of the Personal Data Protection Law essentially establishes a tiered control mechanism for the transfer of personal data abroad. The first requirement is provided in paragraph (2), namely the obligation to ensure that the recipient country has an equivalent or higher level of personal data protection. The second requirement is provided in paragraph (3), namely the obligation to provide adequate and binding personal data protection if the standard under paragraph (2) is not fulfilled. The third requirement is provided in paragraph (4), namely the consent of the data subject as a last resort. This construction shows that the lawmakers have sought to place cross-border data transfers within the framework of prudence and legal protection.

Conceptually, the first requirement under Article 56 paragraph (2) of the Personal Data Protection Law adopts the idea of adequacy as recognized in the international data protection regime. This means that data transfers cannot be regarded merely as technical movements, but must be preceded by an assessment of the ability of the recipient country to guarantee a level of protection that is not lower than the standards under Indonesian law.

From the perspective of legal policy, the regulation of cross-border personal data transfers under Article 56 of the Personal Data Protection Law must also be understood as the state's effort to maintain a balance between the openness of data flows and the protection of national data sovereignty. In the digital era, data is no longer merely information, but a strategic asset that concerns individual interests, economic interests, and even state security. Therefore, the regulation of cross-border personal data transfers should not merely contain permission or prohibition, but must also provide clear requirements regarding the recipient country, the form of legal safeguards, and the party responsible after the transfer has been carried out. Without such clarity, the state risks losing normative control over its citizens' data when personal data is located in another jurisdiction with different protection standards.

The principle of accountability should be an inseparable element of the construction of Article 56 of the Personal Data Protection Law (Tarikh, 2025). The responsibility of the personal data controller should not be understood as ending once the data has been successfully transferred abroad. On the contrary, such responsibility must remain attached as long as the data continues to be processed, used, stored, or further transferred by the recipient in the destination country. Within this framework, accountability is not merely an administrative obligation, but a normative basis for ensuring that data subjects continue to have a party that can be held responsible. When the law has not yet clearly affirmed the limits and forms of such

accountability, the protection of data subjects becomes fragile because the relationship between the legality of the transfer and the continuity of legal responsibility is not formulated clearly.

The requirement of an equivalent level of protection in cross-border personal data transfers is intended to minimize the risk of failure in personal data protection when personal data is transferred to another jurisdiction (Nathasya et al., 2023). Therefore, the recipient country must be able to provide a level of protection equivalent to that of the country of origin so that the rights of data subjects remain protected. Accordingly, the main objective of Article 56 of the Personal Data Protection Law is not merely to regulate the procedure for personal data transfers, but also to ensure the continuity of legal protection for personal data after the data leaves Indonesia's jurisdiction.

The adequacy requirement is not merely an administrative mechanism for authorizing the transfer of personal data to a third country, but a legal instrument aimed at ensuring that the level of personal data protection is maintained after the data is located outside the jurisdiction of the country of origin. Therefore, the recipient country must be able to provide a level of protection that is substantially equivalent to standards regarded as adequate and equivalent, so that the rights of data subjects remain protected. The concept of adequacy functions as an instrument for the continuity of legal protection, not merely as a formal requirement in the implementation of cross-border personal data transfers (Jiménez-Gómez & Sofía, 2021).

Under the first requirement, Article 56 paragraph (2) of the Personal Data Protection Law adopts the concept of adequacy by requiring that the recipient country have a level of personal data protection that is equivalent to or higher than that of Indonesia. Normatively, the adoption of this principle shows that the lawmakers position personal data transfer as a legal act requiring an eligibility assessment of the protection regime in the recipient country. However, a fundamental problem arises because the law does not explain the indicators that must be used to assess the meaning of "equivalent or higher". As a result, this phrase functions only as a general direction of legal policy and has not yet become an operational standard that can be used with certainty by data controllers, law enforcement officials, or supervisory authorities. Without clear normative measures, this first requirement may easily shift into a subjective assessment, thereby weakening the preventive function that Article 56 of the Personal Data Protection Law seeks to establish.

Conceptually, the meaning of "equivalent or higher" should be understood through at least three forms of assessment. First, equivalence at the level of principles, namely whether the recipient country recognizes the basic principles of data protection, such as the legality of processing, purpose limitation, data security, and respect for data subjects' rights. Second, equivalence at the level of rights, namely whether data subjects continue to have a legal standing to obtain information, access, rectify, erase, and seek remedies for the use of their personal data. Third, equivalence at the level of legal safeguards, namely whether mechanisms are available to enforce those rights in the event of a violation. Without affirmation of these assessments, the phrase "equivalent or higher" will remain ambiguous and will not provide certainty as to when a country is truly eligible to become the destination for personal data transfers.

The second requirement under Article 56 is contained in paragraph (3) of the Personal Data Protection Law, namely the obligation to ensure the existence of adequate and binding personal data protection if the recipient country does not meet the equivalence standard under paragraph (2). This provision is important because it shows that failure to meet the first requirement does not automatically preclude a transfer. However, a transfer may only be carried out if another sufficiently strong legal safeguard is available to maintain the continuity of the protection of data subjects' rights. The main problem with paragraph (3) lies in the absence of a normative explanation of the meaning of "adequate" and "binding." The absence of such measures makes this norm vulnerable to broad interpretation, even though,

systematically, paragraph (3) is intended to serve as an alternative legal safeguard when the recipient country has not met the adequacy standard.

Conceptually, the element of "adequate" refers to the sufficiency of the level of legal protection that continues to safeguard the rights of data subjects after the data has been transferred outside Indonesia's jurisdiction, while the element of "binding" refers to the existence of a normative basis that obliges the data recipient to comply with such protection standards. These two elements cannot be separated. A safeguard that is deemed adequate but lacks normative binding force will only produce a formal commitment, while binding force without sufficient substantive protection will not ensure the continuity of the protection of data subjects' rights. In international practice, the need for adequate and binding safeguards is commonly translated into legal instruments with clear forms and binding force, such as standard contractual clauses or binding corporate rules. This illustration shows that the concept under paragraph (3) can essentially be formulated in a more operational manner; the problem is that the Personal Data Protection Law has not yet provided the parameters, forms, and minimum thresholds necessary for its certain application.

The third requirement under Article 56 of the Personal Data Protection Law is contained in paragraph (4), which places the consent of the data subject as the final basis for transfer if the requirements under paragraphs (2) and (3) are not fulfilled. Normatively, this construction raises an important problem. Consent is indeed one of the lawful bases for personal data processing. However, in the context of cross-border transfers, consent cannot replace the need for objective standards that guarantee the quality of protection in the recipient country. If consent is used as a substitute for the non-fulfilment of the requirement of equivalent protection and the absence of adequate and binding safeguards, the control mechanism shifts from structural protection to an individual burden placed on the data subject. In practice, data subjects do not necessarily have the bargaining position, knowledge, or ability to adequately assess cross-jurisdictional risks. Therefore, consent should be understood as a complement to a clear normative structure, not as a means to cover the weaknesses of protection standards that have not been firmly formulated.

When read as a whole, Article 56 paragraphs (2), (3), and (4) of the Personal Data Protection Law establish tiered requirements as a form of preventive legal protection intended to prevent the misuse of personal data before the transfer is carried out. From the perspective of legal policy, this construction reflects the state's effort to balance the need for data flows in the digital economy with the protection of citizens' rights. The recognition of the principle of an equivalent level of protection, adequate and binding safeguards, and consent as a last resort shows that the lawmakers do not regard cross-border personal data transfers as an absolute freedom for data controllers. However, this objective has not been fully achieved at the operational level because each safeguard requirement still leaves ambiguity in its formulation. As a result, the norm that should function as a means of preventive protection has not yet become a firm limit in assessing the legality of personal data transfers abroad.

The Personal Data Protection Law has not yet explained the parameters for assessing the meaning of "equivalent or higher," nor has it explained the form of "adequate and binding personal data protection." As a result, paragraphs (2) and (3) cannot yet fully operate as operational standards. In international practice, such safeguards are commonly embodied in measurable legal instruments, such as standard contractual clauses or binding corporate rules. Meanwhile, paragraph (4), which places the consent of the data subject as the final basis, must also be read carefully because consent cannot replace the need for objective protection standards.

Nevertheless, although the Personal Data Protection Law reflects principles similar to those under the GDPR, particularly through the requirements of an equivalent level of protection, adequate protection, and the consent of the data subject, it has not yet provided clear

standards or explanations for assessing whether the recipient country offers an equivalent level of protection. In addition, the Personal Data Protection Law has not clearly regulated the form or substance of agreements or other legal instruments that may serve as the basis for ensuring personal data protection when the recipient country does not meet the equivalence requirement. Unlike the GDPR, which provides more detailed legal mechanisms and instruments, Article 56 of the Personal Data Protection Law has not yet formulated clear parameters or assessment procedures. This ambiguity may lead to differences in interpretation in the implementation of cross-border personal data transfers and may reduce legal certainty for data controllers in determining whether a transfer has fulfilled the required protection standards (Riswandi & Gultom, 2023).

Although Article 56 of the Personal Data Protection Law has adopted an approach aligned with international standards through the requirements of an equivalent level of protection, adequate protection safeguards, and data subject consent, the provision has not yet fully provided legal certainty in cross-border personal data transfers. The main problem lies in the absence of clear and measurable parameters for assessing the equivalence of the level of data protection in the recipient country, as well as the absence of implementing regulations governing the evaluation and supervision mechanisms (Prastowo et al., 2026). As a result, data controllers face difficulties in determining compliance with the provisions on personal data transfers abroad, while data subjects have not yet obtained adequate assurance regarding the level of protection of their personal data once it is located in another jurisdiction. This condition indicates a gap between the normative construction of Article 56 of the Personal Data Protection Law and the need for legal certainty in the implementation of cross-border personal data transfers.

Other studies have stated that the effectiveness of personal data protection under the Personal Data Protection Law still faces obstacles due to the absence of more detailed regulation through implementing regulations (Alfitri et al., 2024). The absence of such implementing rules creates legal uncertainty because various provisions in the Personal Data Protection Law do not yet have clear operational guidelines for their application. As a result, the application of these provisions may give rise to multiple interpretations and affect the effectiveness of the protection of data subjects' rights. This condition shows that a number of norms in the Personal Data Protection Law remain general and abstract, thereby requiring further regulation in order to provide adequate legal certainty. These findings are relevant to the regulation of cross-border personal data transfers under Article 56 of the Personal Data Protection Law, which also leaves ambiguity regarding the parameters of an equivalent level of protection and adequate protection. Therefore, the norms in the Personal Data Protection Law need to be clarified by regulating the limits and parameters of the requirements for cross-border personal data transfers as part of the substantive scope of statutory law. The formulation of derivative regulations will be difficult if the statute itself does not provide clear normative rules.

Thus, the construction of Article 56 of the Personal Data Protection Law as a control mechanism for cross-border personal data transfers has in fact shown an appropriate regulatory direction because it places cross-border personal data transfers within the framework of preventive protection. The main problem does not lie in the absence of a normative idea, but in the lack of firmness in formulating the measures of equivalent protection, the form of adequate and binding safeguards, and the limits on the use of consent as a last resort. As long as these core concepts have not been formulated more clearly and measurably, Article 56 of the Personal Data Protection Law will remain at risk of becoming a merely declaratory norm that is not yet fully operational. Therefore, the strengthening of this article should be directed not only toward the addition of technical rules, but also toward the affirmation of its normative construction so that the control mechanism can genuinely maintain the continuity of the

protection of data subjects' rights after personal data has moved outside Indonesia's jurisdiction.

The Impact of Normative Ambiguity in Article 56 of the Personal Data Protection Law on Legal Certainty and the Protection of Data Subjects' Rights

The regulation of cross-border personal data transfers under Article 56 of the Personal Data Protection Law still contains normative ambiguity because it does not provide clear definitions or parameters regarding the criteria for an "equivalent level of personal data protection" and "adequate and binding protection" as requirements for transferring personal data abroad (Nafisa et al., 2025). As a result, data controllers do not have definite guidance in assessing the eligibility of the recipient country, while data subjects do not obtain adequate assurance regarding the security of their data once it is located outside Indonesia's jurisdiction. This ambiguity reduces the preventive function of Article 56 of the Personal Data Protection Law in protecting personal data from the risks of misuse, leakage, and weak law enforcement in the recipient country. In addition, this regulation has not fully reflected the principle of transparency because it does not require notification to data subjects in every cross-border personal data transfer, thereby creating problems of legal certainty and the protection of data subjects' privacy rights.

The ambiguity in the formulation of Article 56 of the Personal Data Protection Law has a direct impact on the weakening of legal certainty. Personal data controllers do not obtain definite guidance on when a country may be considered to have an equivalent level of protection, what instruments may be qualified as adequate and binding protection, and how legal responsibility remains attached after data has been transferred abroad. This situation opens room for multiple interpretations, creates inconsistency in implementation, and may allow cross-border personal data transfers to take place without objective protection standards. Legal certainty in personal data protection is not determined merely by the existence of legislation, but also by the completeness of its normative construction, which needs to be regulated in detail and comprehensively (Anjawai et al., 2022).

From the perspective of legal protection, the main problem lies in the continuity of data subjects' rights after the data leaves Indonesia's jurisdiction. The rights to obtain information, access, rectify, erase, restrict processing, and obtain remedies are essentially guaranteed under the Personal Data Protection Law. However, these rights will be difficult to exercise effectively if personal data is transferred to another jurisdiction without clear normative safeguards. A limited comparison with the GDPR shows that the adequacy principle does not stop at the recognition of a term, but is translated into operational mechanisms. Therefore, the strengthening of Article 56 of the Personal Data Protection Law should be directed toward establishing indicators of an equivalent level of protection, affirming the forms of adequate and binding protection instruments, limiting the function of consent as a last resort, and affirming the responsibility of data controllers for the continuity of protection after the transfer has been carried out.

Normative ambiguity in Article 56 of the Personal Data Protection Law does not only create problems at the conceptual level, but also directly affects the quality of legal certainty received by the parties involved in cross-border personal data transfers. Within the framework of the rule of law, legal certainty requires that norms be formulated clearly, consistently, and predictably. If the criteria for determining which recipient countries are deemed to have an equivalent level of protection, the forms of adequate and binding safeguards, and the limits on the use of consent as a last resort are not formulated firmly, personal data controllers do not have sufficient normative guidance to determine lawful conduct. In such circumstances, the legality of personal data transfers becomes dependent on the interpretation of each party rather

than on objective legal standards. This condition weakens the function of law as a guide for conduct and as a limit on actions that may harm data subjects.

From the perspective of legal certainty, the vague formulation of Article 56 of the Personal Data Protection Law creates broad room for multiple interpretations. Data controllers may subjectively assess that a country has fulfilled the standard of equivalent protection, while other parties may reach the opposite conclusion. Similarly, the phrase "adequate and binding protection" may be interpreted loosely as merely an administrative commitment or a unilateral clause that does not genuinely provide normative binding force. As a result, the legal standard that should function as a preventive mechanism turns into an overly broad space of discretion. In this situation, legal certainty is weakened not only for data controllers, but also for data subjects, because they cannot know with certainty the legal basis used when their personal data is transferred outside Indonesia's jurisdiction. Cross-border personal data transfers place data beyond the reach of the law of the originating jurisdiction, thereby creating a regulatory gap in personal data protection (Yadav & Dhawan, 2023). Article 56 of the Personal Data Protection Law should be able to address the regulatory gap that arises when personal data leaves Indonesia's jurisdiction. However, the ambiguity of the parameters concerning an equivalent level of protection may instead reduce the effectiveness of that function.

Legal certainty and legal protection in the context of cross-border personal data transfers are essentially inseparable. Legal certainty is a prerequisite for legal protection to operate effectively. The absence of clear normative parameters causes the provision to open room for multiple interpretations in its application by business actors and regulators, so that it has not yet been able to provide adequate legal certainty (Aulia, 2024). Without a clear formulation of norms, data subjects do not have a definite basis for knowing their rights, the party responsible, or the available remedy mechanisms in the event of data misuse. Therefore, the ambiguity of Article 56 of the Personal Data Protection Law is not merely a matter of wording or legislative technique, but a substantive problem that directly affects the ability of law to protect the rights of data subjects. The more ambiguous the formulation of the norm, the weaker the continuity of legal protection that can be provided once the data has moved outside Indonesia's jurisdiction.

The vulnerability of data subjects becomes greater when data has been transferred to another jurisdiction. At this stage, data subjects may lose practical control over how their data is processed, used, stored, or further transferred to third parties. If the provisions concerning transfer requirements and the forms of protection safeguards are not formulated firmly, the rights of data subjects to obtain information, request access, rectify data, erase data, or seek remedies will be difficult to exercise effectively. In this context, legal protection cannot be measured merely by the existence of a formal prohibition or authorization to transfer personal data, but must be measured by the capacity of the norm to ensure that data subjects' rights remain operational after the transfer has been carried out.

From a human rights perspective, personal data cannot be separated from the right to privacy and the protection of one's person. Therefore, the issue of cross-border personal data transfers is not merely a technical matter of data processing, but concerns the continuity of the protection of citizens' human rights. The 1945 Constitution of the Republic of Indonesia provides a constitutional basis for the protection of the person, security, and property rights, which in the digital context includes personal data attached to individuals. When data is transferred to another jurisdiction without clear protection standards, these constitutional rights may be weakened because the state no longer has effective guarantees to ensure that its citizens' data remains protected. In such circumstances, the normative ambiguity of Article 56 of the Personal Data Protection Law may be viewed as a factor that reduces the state's ability to fulfil its obligation to protect citizens' rights in the digital sphere.

The main risk in cross-border personal data transfers lies in the limitations of jurisdiction and law enforcement. When data is located on servers, systems, or entities subject to the law of another country, the ability of data subjects and the originating state to seek remedies becomes more limited. These obstacles may include differences in legal systems, the absence of effective complaint mechanisms, or the absence of an independent supervisory authority accessible to data subjects. In such conditions, the harm suffered by data subjects is not only potential, but also structural, because their legal position becomes weaker from the outset due to the absence of clear normative safeguards before the transfer is carried out. Therefore, the ambiguity of Article 56 of the Personal Data Protection Law must be understood as a factor that increases the vulnerability of data subjects in cross-jurisdictional legal relations.

Weak personal data protection may cause harm that is not only individual in nature, but also affects public trust in electronic system providers (Putra et al., 2024). Personal data breaches increase the risk of identity theft, misuse of financial information, and threats to the privacy of data owners. In addition, data breach incidents also have implications for the declining integrity of information systems and public trust in institutions that collect and manage personal data. In the context of cross-border personal data transfers, such potential harm may become more complex if data is transferred to a jurisdiction with a lower level of protection, making remedies for data subjects increasingly difficult to obtain.

Regulatory ambiguity also increases the potential for misuse of personal data. Data transferred abroad may be used beyond the original purpose of its collection, analyzed for commercial interests without meaningful consent, traded across platforms, or even leaked due to weak security in the recipient country. This risk becomes even higher in digital ecosystems that process population data, financial data, consumer preferences, location data, and behavioral data with high economic value. If the law does not provide a clear qualification of the protection standards that must be fulfilled before a transfer is carried out, the mechanism for preventing data misuse becomes weak. Thus, normative ambiguity does not only affect formal legal aspects, but also has direct implications for the increased risk of leakage and exploitation of personal data.

The harm suffered by data subjects due to weak protection in cross-border transfers may arise in various forms. From a legal perspective, data subjects may lose their position to control the use of their personal information and suffer violations of their privacy rights. From an economic perspective, misused data may result in fraud, identity theft, account breaches, or forms of commercial exploitation without proper consent. From a social and psychological perspective, data misuse may lead to a loss of security, psychological distress, reputational damage, stigma, and even discrimination if the leaked data relates to sensitive information. Therefore, the impact of normative ambiguity in Article 56 of the Personal Data Protection Law should not be viewed merely as a regulatory problem, but as a problem that may cause real harm to data subjects.

In addition to its impact on individuals, the ambiguity in the regulation of cross-border personal data transfers also has broader public implications. In the digital era, citizens' personal data is not only valuable to individuals, but also has strategic dimensions for the economy, security, and the state's digital sovereignty. The transfer of personal data abroad without clear protection mechanisms may result in strategic data being placed under the control of foreign entities without adequate national supervision. In the long term, this situation may create digital dependency, weaken national data sovereignty, and open space for broader security disturbances. Therefore, the protection of data subjects in cross-border transfers must also be understood as part of the public interest and the interest of the state, not merely as a private matter between data controllers and individuals.

When compared in a limited manner with the European Union data protection regime, it can be seen that legal certainty in cross-border personal data transfers does not stop at the

formulation of principles, but is translated into mechanisms that allow data subjects' rights to remain enforceable. The GDPR recognizes not only the adequacy principle, but also provides complaint channels, compensation, independent supervision, and legal instruments that regulate the responsibilities of the parties concerned. In the Indonesian context, the limitations of the existing regulation show that cross-border data subjects have not yet obtained sufficiently strong guarantees of remedies in the event of a violation. This demonstrates that strengthening Article 56 of the Personal Data Protection Law is not only a matter of clarifying transfer requirements, but also of ensuring the continuity of rights, accountability, and remedies for data subjects after the transfer has been carried out. Thus, the impact of normative ambiguity in Article 56 of the Personal Data Protection Law operates in two dimensions at once. In the first dimension, such ambiguity weakens legal certainty because data controllers, data subjects, and state authorities do not have firm normative guidance for assessing the legality of cross-border personal data transfers. In the second dimension, such ambiguity weakens legal protection because the rights of data subjects become difficult to maintain effectively after the data moves to another jurisdiction. Therefore, the strengthening of Article 56 of the Personal Data Protection Law should be directed not only toward clarifying key terms, but also toward building a stronger relationship between transfer requirements, data controller responsibility, the continuity of data subjects' rights, and remedy mechanisms that can operate in a cross-border context.

The impact of normative ambiguity can also be seen in the declining legal compliance of the parties involved in cross-border personal data transfers. Vague norms not only complicate law enforcement, but also reduce compliance incentives because actors do not have a clear understanding of the obligations that must be fulfilled or the legal consequences that may arise. In such conditions, law loses its function as a guide for conduct. In the context of personal data transfers, compliance depends heavily on the existence of firm parameters concerning transfer requirements, the forms of protection that must be available, and the obligations of data controllers when a violation occurs. The more unclear the applicable norm, the greater the space for transfers to be carried out merely on the basis of internal assessment or business interests.

At the level of repressive protection, the weakness of the norm in Article 56 of the Personal Data Protection Law also has implications for the difficulty of establishing an effective remedy mechanism. When data is already located in the recipient country and misuse occurs, data subjects often face obstacles in accessing dispute resolution institutions, filing complaints, or claiming compensation. These obstacles arise not only because of jurisdictional differences, but also because the law has not clearly affirmed how the relationship between data controllers in Indonesia and recipients abroad must be maintained for the purposes of remedies. As a result, the right to remedy formally recognized by the Personal Data Protection Law may become difficult to exercise in a cross-border context if it is not supported by a firm normative basis concerning responsibility and enforcement mechanisms.

Although Law Number 27 of 2022 on Personal Data Protection has been enacted, personal data protection in Indonesia still faces various challenges that hinder the realization of effective legal protection. One of the main problems is the continuing normative ambiguity that causes the regulation of personal data protection to remain not fully comprehensive, particularly in relation to the requirements for transferring personal data abroad and the guarantee of the level of protection for data processed outside Indonesia's jurisdiction (Judijanto, L., & Nugroho, 2025). This condition creates vulnerability to the misuse of personal data and shows that the existing regulation has not fully provided legal certainty or guaranteed the protection of data subjects' privacy rights. Therefore, Article 56 of the Personal Data Protection Law still requires clearer normative formulation so that the mechanism for cross-border personal data transfers can be applied firmly.

Several studies have identified that one of the problems in Law Number 27 of 2022 on Personal Data Protection is the incompleteness of derivative regulations governing the technical implementation of the law (Ayiliani & Farida, 2024; Fitriana & Nur, 2026; Prastowo et al., 2026). Nevertheless, this problem cannot be viewed solely as a consequence of the absence of implementing regulations, but must also be linked to the normative construction of the statute itself. Norms that remain general and do not provide clear parameters cause the drafters of implementing regulations to lack an adequate normative basis for formulating detailed technical provisions. In the context of Article 56 of the Personal Data Protection Law, the phrases "equivalent level of protection" and "adequate protection" have not been accompanied by indicators or assessment mechanisms that can serve as guidance in drafting implementing regulations. As a result, regulators face difficulty in formulating technical provisions without potentially expanding or adding normative substance that should have been established at the statutory level. Thus, the absence of implementing regulations does not only reflect an implementation problem, but also indicates a weakness in the normative construction of Article 56 of the Personal Data Protection Law, which has not yet provided a sufficiently clear legal basis for further regulation. The absence of implementing government regulations is a consequence of the ambiguity in the normative construction of Article 56 of the Personal Data Protection Law.

Law Number 27 of 2022 on Personal Data Protection still requires the support of comprehensive implementing regulations and a supervisory authority with the power to oversee the implementation of personal data protection (Hockop, 2024). The existence of these two instruments is important to provide technical guidance, ensure the compliance of data controllers, and guarantee the effectiveness of law enforcement in the implementation of cross-border personal data transfers. Nevertheless, the formulation of implementing regulations and the strengthening of supervisory functions must be based on a clear statutory norm. In the context of Article 56 of the Personal Data Protection Law, the phrases "equivalent level of protection" and "adequate protection" are still not accompanied by adequate parameters or assessment mechanisms. This condition causes both the drafters of implementing regulations and supervisory authorities to lack a sufficient normative basis for formulating operational standards and carrying out supervisory functions consistently. Therefore, the strengthening of implementing regulations and institutions should begin with the refinement of the normative construction of Article 56 of the Personal Data Protection Law, so that a clear legal basis is available for the regulation and supervision of cross-border personal data transfers.

For this reason, the reformulation of Article 56 of the Personal Data Protection Law should be directed toward the formulation of terms that are more operational and testable in their application. The phrases concerning an equivalent or higher level of protection, adequate and binding protection, and consent as a last resort must be translated into assessable indicators, verifiable instruments, and enforceable responsibilities. This reformulation is important so that Article 56 of the Personal Data Protection Law does not merely reflect the legal policy intention to protect citizens' personal data, but genuinely functions as a norm that provides legal certainty and legal protection effectively in the practice of cross-border personal data transfers.

CONCLUSION

The normative problem concerning the requirements for cross-border personal data transfers under Article 56 of the Personal Data Protection Law lies in the lack of firmness in the normative construction of the three transfer requirements, namely an equivalent or higher level of protection, adequate and binding protection, and the consent of the data subject as a last resort. These provisions have demonstrated a preventive protection approach to the transfer of personal data abroad, but they have not yet provided sufficiently clear normative parameters for determining the standard of equivalent protection, the form of adequate and binding

safeguards, or the limits on the use of consent. Thus, in relation to the objective of analyzing the normative construction of Article 56 of the Personal Data Protection Law, this study finds that the provision still requires normative clarification in order to prevent differences in interpretation.

The normative ambiguity of Article 56 of the Personal Data Protection Law has implications for the weakening of legal certainty and the protection of data subjects' rights. Personal data controllers do not obtain definite guidance in assessing the eligibility of the recipient country or determining the protection instruments that must be used, while data subjects face greater vulnerability because their rights become more difficult to enforce once the data is located outside Indonesia's jurisdiction. Therefore, the findings of this study answer the second research objective by showing that normative clarity in Article 56 of the Personal Data Protection Law is a prerequisite for the continuity of legal protection, the accountability of personal data controllers, and legal certainty in cross-border personal data transfers.

Accordingly, Article 56 of the Personal Data Protection Law needs to be clarified with respect to the indicators of an equivalent level of protection, the forms of adequate and binding protection, the limits on the use of data subject consent, and the continuity of the responsibility of personal data controllers after the transfer has been carried out. Such clarification is necessary so that the regulation of cross-border personal data transfers under the Personal Data Protection Law can provide legal certainty while ensuring the protection of data subjects' rights through a clear and conceptually adequate legal framework.

REFERENCE

Alfitri, N. A., Rahmawati, & Firmansyah. (2024). Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Journal Social Society*, *4*(2), 92–111. https://doi.org/https://doi.org/10.54065/jss.4.2.2024.511

Anjawai, N. B., Amboro, F. Y. P., & Hutauruk, R. H. (2022). Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*, *4*(2), 207–218. https://doi.org/10.37680/almanhaj.v4i2.1791

Aulia, E. (2024). Analisis Pasal 56 dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Review Unes*, *7*(1), 225–240. https://review-unes.com/index.php/law/article/download/2267/1861/

Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai UpayaPelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, *6*, 431–455.

Charles, M., & Oktawijaya, N. (2026). Quo Vadis Urgensi Pembentukan Otoritas Independen atas Kesepakatan Transfer Data Pribadi Warga Indonesia ke Amerika Serikat. *Beleid: Journal of Administrative Law and Public Policy*, *4*(1), 140–154.

Fitriana, S. A., & Nur, H. (2026). Analisis Yuridis Normatif Perlindungan Data Pribadi Di Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Hukum dan Kewarganegaraan*, *16*(7), 2041–2050. https://doi.org/https://doi.org/10.6679/rw94sy93

Gregory, V. W. (2022). Cross-Border Data Flows, the GDPR, and Data Governance. *International Organisations Research Journal*, *17*(1). https://doi.org/10.17323/1996-7845-2022-01-03

Hadjon, P. M. (1987). *Perlindungan Hukum Bagi Rakyat Indonesia*. PT Bina Ilmu.

Hockop, S. P. (2024). Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR). *Jurnal Esensi Hukum*, *6*(2), 105–124.

Jiménez-Gómez, & Sofía, B. (2021). Cross-Border Data Transfers Between the Eu and the U.S.: a Transatlantic Dispute. In *Santa Clara J. Int'l L.* (Vol. 19, Nomor 2).

Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum Dan HAM*, *3(03)*, 118–124. https://doi.org/https://doi.org/10.58812/shh.v3i03.544

Jurcys, P., Compagnucci, M. C., & Fenwick, M. (2022). The Future of International Data Transfers : Managing New Legal Risk with a 'User-Held' Data Model. *The Computer Law and Security Review*, *46*.

Manullang, E. F. M. (2017). *Legisme, Legalitas dan Kepastian Hukum* (Cetakan ke). Kencana.

Maramis, J. J., Koesoemo, A. T., & Pinasang, B. (2024). Analisis Yuridis Perlindungan Data Pribadi Dalam Transaksi Pinjaman Online. *Jurnal Fakultas Hukum Unsrat*, *13*(2), 1–11. https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/53924

Nafisa, T. A., Alam, M. Z., & Maharani, D. P. (2025). Analisis Pengaturan Pengalihan Data Pribadi Lintas Negara Akibat Akuisisi dalam Undang Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Jurnal Dialektika Hukum*, *7*(1), 97–135.

Nathasya, S. N., Rosadi, S. D., & Pratama, G. G. (2023). *Studi Komparasi Pelindungan Data Pribadi Warga Negara Indonesia Dalam Transfer Data Pribadi Lintas Batas (Transborder Personal Data Transfer) Antara Indonesia Dengan Jepang*. *7*(3), 324–335.

Prastowo, A. A., Algamar, A. F., & Siahaan, G. Y. (2026). *Kepastian Hukum dalam Transfer Data Lintas Negara: Tinjauan Terhadap Undang-Undang Perlindungan Data Pribadi di Indonesia*. *4*(2), 97–135. https://doi.org/https://doi.org/10.61104/alz.v4i2.5760

Putra, R. K., Fahmi Idris, M., & Widhiati, G. (2024). Perlindungan Data Pribadi Dalam Era Big Data : Implikasi Hukum Di Indonesia. *Jurnal Kajian Ilmu Hukum dan Politik*, *2*(4), 31–44. https://journal.stekom.ac.id/index.php/Jaksa

Riswandi, B. A., & Gultom, A. M. (2023). Protecting Our Mosts Valuable Personal Data: a Comparison of Transborder Data Flow Laws in the European Union, United Kingdom, and Indonesia. *Prophetic Law Review*, *5*(2), 179–206. https://doi.org/10.20885/PLR.vol5.iss2.art3

Tarikh, A. (2025). *Analisis Perbandingan Hukum Perlindungan Data Antara Indonesia Dan Uni Eropa: Tinjauan Kasus Cambridge Analytica*. *2*(27), 1–16.

Tjatur, H., C., D. I., Wardhana, B., & Riyanto, G. D. (2024). *Pelindungan Data Pribadi Dalam Jurnalisme Dan Media*. 165.

Tomasoa, G. O. (2024). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Pada Platform Media Sosial. *PAMALI: Pattimura Magister Law Review*, *4*(1), 24. https://doi.org/10.47268/pamali.v4i1.1363

Yadav, T. P., & Dhawan, A. S. (2023). Cross-Border Data Transfers: Legal Framework And Challenges. *International Journal of Arts & Education Research*, *12*(6), 118–133.