PROTECTION OF DATA SUBJECT RIGHTS IN THE TRANSFER OF PERSONAL DATA BETWEEN DATA CONTROLLERS IN INDONESIA: A COMPARATIVE ANALYSIS OF THE PDP LAW AND THE EU GDPR

Syahreza Fachran[1*], Sinta Dewi Rosadi[2], Prita Amalia[3]
[1,2,3]Faculty of Law, Universitas Padjadjaran, Sumedang, Indonesia
syahreza21001@mail.unpad.ac.id[1*], sinta@unpad.ac.id[2], prita.amalia@unpad.ac.id[3]

Abstract

The rapid digital transformation and growth of e-commerce in Indonesia have triggered a high volume of personal data transfers between controllers. while Article 55 of the Personal Data Protection Law (UU PDP) provides only a general authorization without clear technical guidance, creating legal uncertainty and risks to data subject rights. This study analyzes the legal uncertainty of UU PDP's regulation of controller-to-controller data transfers compared to the EU GDPR and proposes an accountable and transparent mechanism tailored to Indonesia. A normative and comparative legal method is employed, examining legislation, the principles of transparency and accountability, and a comparison between Article 55 UU PDP and Article 46 GDPR on safeguards and Standard Contractual Clauses (SCCs). The findings reveal substantial gaps in technical standards, verification mechanisms, documentation, and enforcement, in contrast to the GDPR's modular SCCs, mandatory DPIAs, records of processing activities, and effective supervisory powers. The absence of standardized contractual clauses and an operational supervisory authority in Indonesia weakens transparency and the fulfillment of data subject rights. The study recommends adopting Indonesia-specific SCCs, strengthening an independent supervisory authority, and implementing techno-regulation through privacy by design, encryption, and Data Loss Prevention. Harmonization with GDPR standards via SCCs and institutional strengthening is essential to ensure secure, transparent, and accountable controller-to-controller transfers.

Keywords: Data Subject; Data Controller; Personal Data Protection; Personal Data Transfer; Standard Contractual Clauses.

INTRODUCTION

Indonesia has entered an era of digital transformation marked by rapid growth in internet users. Based on the latest data from the Indonesian Internet Service Providers Association (APJII), the number of internet users in Indonesia in 2024 will reach 225 million people out of a total population of 278.7 million, or equivalent to a penetration rate of 80.7% (Dwi Jamitko, 2024). This figure shows a consistent increase from the previous year, which reached 221.5 million users or 79.5% of the total population. This data demonstrates that nearly 8 out of 10 Indonesians are connected to the internet and engaged in digital activities that enable the massive collection, processing, and transfer of personal data (APJII, 2024).

This digital transformation is further strengthened by the dominance of millennials and Gen Z, who are the largest internet users in Indonesia. Generation Z (born 1997-2012) accounts for 34.4% of total internet users, while millennials (born 1981-1996) contribute 30.62% (Farhan Kalyara, 2024). These two generations are very active in using digital platforms for various purposes, ranging from social media, e-commerce, digital financial services, to electronic government platforms, which indirectly create digital footprints containing large amounts of personal data. The phenomenon of Indonesia's digital economy growth reached USD 82 billion in 2023 and is projected to rise to USD 146 billion in 2025 (Rahmawati, R., & Nurcahyani, N, 2024).

This shows that personal data has become a very valuable asset in the digital ecosystem. Every digital transaction, from online payments, the use of e-commerce applications, to digital government services, involves the collection and processing of personal data which can then be transferred between data controllers for various business and operational purposes. The increase in the digital activities of the Indonesian people is directly proportional to the risk of misuse and leakage of personal data. It should be noted that the protection of personal data is an important part of human rights guaranteed in Article 28G paragraph (1) of the 1945 Constitution regarding personal protection (Matthew, J, et al., 2025). Therefore, the Indonesian government responded to this urgency by passing Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) on October 17, 2022, as a strategic step to protect the digital privacy rights of citizens, one of which discusses the regulation of personal data transfer in Indonesia (Nathasya, S. N, et al., 2025). Although the PDP Law has provided a comprehensive legal framework for personal data protection, there is legal uncertainty in the regulation of personal data transfers between data controllers within Indonesia. Article 55 of the PDP Law explains that "Personal Data Controllers may transfer Personal Data to other Personal Data Controllers within the jurisdiction of the Republic of Indonesia". Article 55 of the PDP Law currently only stipulates general permission for data controllers to transfer personal data between data controllers within the jurisdiction of the Republic of Indonesia without providing clear technical guidelines, thus creating legal uncertainty and weakening the position of data subjects. Without provisions on mandatory encryption mechanisms or security protocols, each controller can use different standards, resulting in a high risk of data leakage or misuse that is difficult to account for. This is in contrast to Article 56 of the PDP Law, which regulates cross-border transfers with the requirement of a level of protection equivalent to that of the PDP Law and the explicit consent of the data subject. Thus, Article 55 needs to be supplemented with implementing regulations that outline security standards, documentation procedures, and verification mechanisms so that data transfers between controllers can take place in a secure, transparent, and accountable manner.

The urgency of regulating personal data transfers between data controllers in Indonesia is increasingly apparent with the rapid digital transformation in the rapidly growing e-commerce sector. Indonesia's e-commerce transaction value is recorded at IDR 487 trillion in 2024, which has contributed significantly to the digital economy with a Gross Merchandise Value (GMV) of $65 billion (Agnes Z, 2025). In addition, the number of e-commerce users in Indonesia is estimated to reach 65 million people in 2024, a significant increase from 38 million users in 2020, and is projected to continue to grow to 99 million users by 2029 (Ramadhani, W. K. S., & Wiraguna, S. A., 2025). The phenomenon of personal data transfer between data controllers in Indonesia can be seen in the privacy policies of e-commerce applications such as Tokopedia, Shopee, and Bukalapak, which clearly state that they will transfer users' personal data to various partners or third parties, including logistics partners such as JNE, J&T, and SiCepat, as well as financial technology companies such as OVO, Gopay, and DANA. In conducting transactions and processing deliveries, this creates a layered flow of personal data transfer that begins when the buyer clicks the "checkout" button, payment verification, processing at the warehouse, to delivery by logistics partners. At each stage, identity, contact details, real-time location, transaction history, and financial details are transferred to a number of different data controllers, creating opportunities for unauthorized access, duplicate storage, and *beyond-purpose* actions (use beyond the original purpose) that are prone to misuse (Nafi'ah, R., 2020). Without transparent and accountable regulations governing data transfers between data controllers within the country and without mandatory

audits by the Personal Data Protection Agency, there is an increased risk of personal data misuse that could harm data subjects and violate their rights as protected by the PDP Law.

In terms of personal data protection, Indonesia often refers to regulations in the European Union, namely the European General Data Protection Regulation (EU GDPR). The EU GDPR strictly regulates the standards for personal data transfers between data controllers, as stipulated in Article 46, which mandates the application of Standard Contractual Clauses (SCCs) as a data protection mechanism in the personal data transfer process (Bradford, et al., 2021). SCCs are model contract clauses that regulate personal data transfers for European Union countries. Indonesia can adopt and adapt the SCCs framework to regulate the transfer of personal data between data controllers in Indonesia, by adjusting it to the legal context and characteristics of Indonesia's personal data protection system. The implementation of a similar mechanism will provide legal certainty and adequate protection for personal data subjects in every data transfer activity. Adequate regulation of personal data transfers between data controllers is essentially a manifestation of the protection of personal data subjects. The PDP Law recognizes the fundamental rights of personal data subjects in Articles 5 to 14 of the PDP Law, which include the right to know the purpose of processing, the right of access, the right of correction, the right of deletion, and the right to data portability (Rosadi, S. D., 2023). However, the protection of these rights is not optimal if there are no clear regulations on how personal data is treated when it is transferred between controllers within the territory of Indonesia.

In the context of personal data transfer, personal data subjects have the right to know to whom their data will be transferred, the purpose of the transfer, how long the data will be stored, and how the data will be protected during the transfer process. Without adequate regulations, personal data transfer can become a loophole that allows for data misuse and violation of data subject rights. Comprehensive personal data transfer regulations will also strengthen the principle of *accountability,* which is one of the fundamental pillars of personal data protection. Data controllers will have a clear obligation to ensure that every transfer of personal data is carried out with the same or higher protection standards, so that the rights of personal data subjects remain guaranteed throughout the data life cycle (Pradana, M. A. E., & Saragih, H, 2024). As a best practice, the principle of data minimization should also be applied, which is to transfer only the minimum amount of data that is absolutely necessary for a specific purpose in order to minimize the risk of leakage. For example, in cross-border health data transfers, data controllers will only send medical information relevant to diagnosis or research, without including complete identity data if it is not necessary (Andanda, P., & Mlotshwa, L, 2024).

Then, looking at the Schrems II case in the European Union shows the consequences if data transfer is carried out without adequate protection. The European Court of Justice invalidated the Privacy Shield because it did not guarantee the protection of EU citizens' data from access by US government authorities, thus emphasizing the need for SCCs and contextual transfer risk assessments. This case serves as an important lesson for every country, including Indonesia, to require audits and protection assessments before transferring personal data. (Murphy, M. H, 2022). Furthermore, clear regulations on personal data transfers will support the implementation of the accountability principle in Article 5 of the PDP Law, which requires data controllers to be able to actively prove legal compliance. However, without rules requiring audit documentation or maintenance of data processing records (records of processing activities), this principle is difficult to implement. The EU GDPR addresses this by requiring SCCs as part of accountability by design as mandated in Article 46 of the EU GDPR (Fernández, A.M, 2019), while Article 55 of the PDP Law does not clearly regulate the process of personal data transfer. As a result, the information and transparency gap between data controllers and data subjects is widening, as the public currently has no access to verify this in Indonesia. With strict regulations in place, data transfers can only be carried out for specific, legitimate purposes that have been approved by the personal data subjects and are supervised by the Personal Data Protection Agency in Indonesia.

This study highlights the urgency of regulating the transfer of personal data between data controllers in Indonesia, in line with the rapid digital transformation in the country. The increasing use of the internet has resulted in a huge volume of personal data that requires stronger protection. The rapid growth of *e-commerce*, with more than 65 million active users in 2024, has triggered the transfer of personal data to various parties, including logistics companies that play a role in the distribution of goods. For example, e-commerce companies such as Tokopedia and Bukalapak transfer their users' personal data to logistics companies and financial technology companies to process shipments and financial transactions carried out on their e-commerce platforms.

Based on the above explanation, it is clear that the urgency of regulating the transfer of personal data between data controllers in Indonesia arises because there is legal uncertainty in Article 55 of the PDP Law regarding the mechanism for transferring personal data between data controllers within the territory of Indonesia. To address this regulatory gap, this study proposes the adoption of SCCs as

stipulated in the EU GDPR as a comprehensive technical reference that has proven to be effective. By adopting SCCs, Indonesia can establish a clear contractual framework to ensure security, confidentiality, and accountability in every process of personal data transfer between data controllers.

As an implementation step, it is also necessary to establish a Personal Data Protection Agency responsible for formulating and issuing technical standards for data transfer based on SCCs, as well as monitoring and enforcing compliance with the application of these clauses. The Personal Data Protection Agency will act as an independent authority that oversees the entire data transfer cycle, from planning to compliance evaluation, so that legal certainty and the protection of personal data subjects' rights can be fully realized in Indonesia.

It can therefore be concluded that the identification of issues in this paper focuses on two main aspects that are highly relevant to the regulation of personal data transfers between data controllers in Indonesia. First, the regulation of personal data transfers between data controllers in Indonesia according to the positive law currently in force, namely the PDP Law, and how the regulation compares to the regulations applied in the European Union through the EU GDPR. Second, an analysis of the personal data transfer process that is adequate and can ensure the protection of the interests of personal data subjects involved in data transfer activities between data controllers. Understanding the appropriate mechanisms for personal data transfer is very important, especially to prevent data leaks and misuse of personal data that could harm the personal data subjects. The urgency of clear and detailed regulations related to the personal data transfer process is crucial to maintain the security and privacy of personal data subjects, as well as to increase public trust in the transparent and accountable management of personal data in Indonesia.

RESEARCH METHOD

The research in this study applies both normative legal and comparative methods, which mutually reinforce one another in examining the urgency of regulating personal data transfers between data controllers in Indonesia. The normative legal method refers to a legal research approach that focuses on library-based or secondary data analysis, encompassing primary, secondary, and tertiary legal materials (Amirudin, 2003). This approach is often called the statute approach, as it involves a detailed review of laws and regulations relevant to the legal issues under study (Soerjono Soekanto, 2008). In this research, several theoretical and normative foundations are employed, such as Lawrence Lessig's techno-regulation theory (Gavaghan, C., 2017), as well as the principles of legal certainty, accountability, and transparency. Additionally, the study draws on the PDP Law and the EU GDPR as the primary regulatory frameworks, alongside other principles and legal norms pertinent to the urgency of governing personal data transfers between data controllers in Indonesia. Consequently, the use of the normative juridical approach provides a strong methodological foundation for analyzing this regulatory necessity.

Then, the comparative research method is an approach carried out by comparing one regulation with another. The comparative method is used to complement the discussion and draw conclusions. This approach is carried out by describing the legal regulations in other countries studied in resolving the legal issues that are the subject of this research (Eberle, E. J, 2011). In conducting this comparative research, the author compares the regulations on personal data transfer between the PDP Law and the EU GDPR. In the comparative research method between the PDP Law and the EU GDPR, Article 46 of the EU GDPR will be compared with Article 55 of the PDP Law, which essentially explains that in the EU GDPR, the regulation of personal data transfer refers to SCCs and becomes the standard for personal data transfer processes in the European Union. whereas Article 55 of the PDP Law does not explain how the transfer of personal data between data controllers in Indonesia can be carried out, thus creating legal uncertainty regarding the regulation of personal data transfer in Indonesia. Therefore, the comparative research method between the PDP Law and the EU GDPR can be a solution to determine that the EU GDPR has regulated the transfer of personal data between data controllers, which can be adopted by Indonesia to ensure the protection of personal data subjects in Indonesia.

RESULT SAND DISCUSSION

Comparison of Personal Data Transfer Regulations between Data Controllers in the PDP Law and the EU GDPR and the Implementation of the Principles of Transparency, Accountability, and Protection of Personal Data Subject Rights in Indonesia

Indonesia's digital transformation has experienced remarkable growth in recent years, particularly through the expansion of the *e-commerce* sector, which has recorded phenomenal growth. Recent data shows that the Indonesian *e-commerce* market will reach a value of USD 75 billion in 2024 with a very optimistic growth projection of up to USD 125 billion in 2027, equivalent to an annual growth

rate (CAGR) of 19% (Lusa, S et al., 2024). This phenomenon is driven by the increasing number of e-commerce users, which is estimated to reach 99 million by 2029, making Indonesia a dominant force in the Southeast Asian digital market with platforms such as Shopee, Bukalapak, Tokopedia, and Blibli leading the electronic trading ecosystem (Khira Ummah, 2024). In this context, the volume of personal data transfers between various data controllers has increased significantly, particularly from *e-commerce* platforms to logistics companies, financial institutions, and other business partners for integrated operational purposes.

The complexity of Indonesia's digital ecosystem creates new challenges in personal data management and protection, where customer information is often transferred through various stages of business processes involving multiple data controllers. This condition is exacerbated by the vulnerability of data protection systems, as evidenced by various cases of massive data leaks involving the largest *e-commerce* platforms in Indonesia. The leak of 91 million Tokopedia accounts in July 2020, the leak of 13 million Bukalapak accounts in 2019, and various other similar incidents provide a clear picture of the risks that lurk in the transfer of personal data between data controllers when protection and supervision standards are still inadequate (Ardika, I. W. C, 2025).

These data breaches highlight the urgency of strengthening the implementation of data subjects' rights, which encompass a comprehensive spectrum of protection. These fundamental rights include the right to transparent notification regarding the purpose and method of data processing, the right of access to obtain copies of personal data, the right to correct inaccurate data, the right to delete data in certain situations, the right to restrict and refuse data processing, the right to data portability, and the right not to be subject to automated decision-making (Mutiara, U., & Maulana, R, 2020). In a comparative context, the PDP Law provides a comprehensive legal framework to protect the rights of data subjects, while the European Union has implemented the EU GDPR, which is recognized as the gold standard in personal data protection globally.

An in-depth comparison between the provisions on personal data transfer in the PDP Law and the EU GDPR reveals substantial differences in approach, mechanism details, and practical implementation. Article 55 paragraph (2) of the PDP Law regulates the transfer of personal data within the jurisdiction of the Republic of Indonesia with relatively simple provisions: "Personal Data Controllers who transfer Personal Data and those who receive the transfer of Personal Data are required to protect Personal Data as referred to in this Law." This formulation does not provide a clear legal basis and does not provide parameters regarding the verification mechanism and the details of the data transfer process.

In contrast, Article 46 of the GDPR adopts a much more structured and comprehensive approach in regulating "*Transfers Subject to Appropriate Safeguards". This provision states: "In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."* Article 46 then provides an *exhaustive* list of *appropriate safeguards* that can be used without requiring specific authorization from the supervisory authority, including (a) legally binding instruments between public authorities, (b) *binding corporate rules* pursuant to Article 47, (c) *standard data protection clauses* adopted by the European Commission, (d) *standard data protection clauses* adopted by a supervisory authority and approved by the Commission, (e) *approved codes of conduct* with binding commitments, and (f) *approved certification mechanisms* with binding commitments.

The fundamental difference lies in the level of specification and *guidance* provided. While Article 55 of the PDP Law provides a relatively open *framework* that relies on implementing regulations for details of implementation, Article 46 of the GDPR provides a very specific and *actionable* mechanism that can be directly implemented by data controllers without waiting for additional regulations. The advantage of the GDPR approach is evident in the availability of approved SCC templates that can be used immediately to facilitate data transfers with adequate protection for personal data subjects.

An analysis of the implementation of the principle of transparency in the practice of personal data transfer shows a significant gap between *e-commerce* platforms in Indonesia and the European Union. The GDPR requires a very detailed level of transparency by requiring data controllers to provide comprehensive information to data subjects on every aspect of data processing and transfer, including the specific identity of the transfer recipient, the purpose and legal basis of the transfer, the risks that may arise, the duration of data storage, and concrete procedures for exercising data subjects' rights. Implementation in the European Union generally includes very detailed *privacy notices* (Morić Z et al, 2024).

Conversely, analysis of *the privacy policies* of Indonesian *e-commerce* platforms shows that the implementation of transparency is still normative and general in nature, resulting in a lack of

transparency in the process of transferring personal data between data controllers. Most *privacy policies* use ambiguous language, such as Shopee's *privacy policy*, which states in point 8.1 that "*In conducting our business, we may need to use, process, disclose, and/or transfer your personal data to third-party service providers, agents and/or affiliates or related companies, and/or other third parties, which may be located in Indonesia or outside Indonesia, for one or more of the Purposes mentioned above. These third-party service providers, agents and/or affiliates or related companies and/or other third parties will process your personal data on our behalf or on behalf of other parties, for one or more of the Purposes mentioned above.*" without providing specific information about the identity of the partners, the purpose of the transfer, the protection mechanisms applied, or the procedures that users can take to control such transfers. This situation is exacerbated by the lack of adequate *guidance* or *privacy policy* templates from Indonesian supervisory authorities, unlike practices in the European Union where data protection authorities provide very detailed templates and guidance. For example, one of the largest *e-commerce* companies in the European Union, Shopify, clearly and explicitly states in its *privacy policy: "We protect your information from others. If a third party requests your personal information, we will refuse to share it unless you give us permission or we are legally required to do so. When we are legally required to share your personal information, we will tell you in advance, unless we are legally forbidden to do so."*

The principle of accountability in the transfer of personal data between data controllers finds different implementations between the PDP Law and EU GDPR *frameworks*. The EU GDPR implements a very strict principle of accountability by requiring data controllers to be able to demonstrate their compliance with all regulatory provisions through complete documentation, conducting *Data Protection Impact Assessments (*DPIA) for high-risk transfers, and appointing *Data Protection Officers* (DPOs) to handle specific cases (Pradana, M. A. E., & Saragih, H, 2024). The accountability mechanism in the EU GDPR also includes the obligation to report data breaches within 72 hours, conduct periodic audits, and maintain comprehensive records of processing activities (Marelli, M, 2024).

The PDP Law adopts similar accountability principles but with implementation mechanisms that still require substantial strengthening. The principle of accountability in the PDP Law is reflected in the obligation of data controllers to implement adequate technical and organizational measures, conduct personal data protection impact assessments, and report incidents to the competent authorities. However, practical implementation faces challenges due to the lack of clear technical standards on how personal data transfer processes are carried out, operationalizable DPIA templates, or systematic audit mechanisms by personal data protection agencies (Pradana, M. A. E., & Saragih, H, 2024).

The *enforcement* aspect also shows significant differences. The EU GDPR gives *data protection authorities* extensive powers to conduct investigations, audits, and law enforcement with administrative sanctions (Gumzej, N., 2023). In contrast, the *enforcement* mechanism of the PDP Law is still in the formative stage with a supervisory agency that has not yet been established and a sanction mechanism that has not been tested in practice.

The use of SCCs as a protection mechanism in personal data transfers shows significant advantages over the PDP Law. The EU GDPR provides modernized SCCs that can be used directly by data controllers to facilitate data transfers with adequate protection. The EU GDPR SCCs have a modular structure that can be adapted to various transfer scenarios, especially between personal data controllers, equipped with detailed *annexes* regarding the description of the transfer, a list of parties and their respective roles, *categories of data subjects* and *personal data, sensitive data measures,* and *technical and organizational measures* (Phillip Lee, 2021).

The advantage of the EU GDPR SCCs also lies in the *transfer impact assessment* mechanism, which requires parties to conduct a comprehensive assessment of the specific circumstances of the transfer, the data controller being transferred to, and the additional *safeguards* needed to protect personal data. This mechanism provides a clear *framework* for assessing risks and implementing appropriate mitigations, including in situations where third parties may access the transferred data and where there are *beyond-purpose* actions (use beyond the original purpose) by third parties (Bradford, L., 2021).

Conversely, the PDP Law does not yet provide SCC templates or adequate *guidance* for practical implementation. Although Article 55 paragraph (2) states that "Personal Data Controllers who transfer Personal Data and those who receive the transfer of Personal Data are required to protect Personal Data as referred to in this Law," this paragraph does not contain clear parameters regarding the minimum content that must be included in data transfer contracts or mechanisms for evaluating the adequacy of such protection. This condition creates uncertainty for data controllers who need to transfer data between data controllers and has the potential to result in inconsistent or inadequate protection

for personal data subjects. Furthermore, this uncertainty does not demonstrate the application of the principles of transparency and accountability.

A comparison of the protection of data subject rights in the context of personal data transfers shows that although the PDP Law and the EU GDPR regulate fundamentally similar rights, there are significant differences in scope, implementation details, and *enforcement* mechanisms. The EU GDPR provides very comprehensive rights, including *the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object,* and *rights related to automated decision making* (Wright, A. & Goodwin, P., 2021). In the context of data transfers, the EU GDPR specifically requires data controllers to provide detailed information about each transfer involving data subjects, including the identity *of recipients,* the *safeguards* applied, and the mechanisms for exercising their rights with the data controller or third party.

The PDP Law regulates the rights of data subjects, which include the right to know the purpose and method of data processing, the right to access and obtain copies of data, the right to correct incorrect data, the right to delete data in certain situations, the right to restrict and refuse data processing, and the right to data portability (Putri, N. M. D. G., et al., 2024). However, the practical implementation of these rights in the context of data transfer still faces challenges due to the lack of clear mechanisms for data subjects to exercise their rights when their data has been transferred to third parties. A significant difference also lies in the *remedy* and *complaint* mechanisms. The EU GDPR provides a very definite mechanism through independent *data protection authorities* with broad investigative powers, as well as the right of data subjects to file *complaints* and obtain *judicial remedies.* In contrast, the *complaint* and *remedy* mechanisms in the PDP Law are still in the process of being established, with the supervisory agency not yet fully operational.

A comprehensive analysis comparing the PDP Law and the EU GDPR in regulating the transfer of personal data between data controllers shows that although *the* fundamental *frameworks* of the two regulations share similarities in their basic principles, there are significant gaps in terms of implementation details, *enforcement* mechanisms, and operational *guidance*. The main gaps include (1) the unavailability of standard contractual clauses or contract templates that can be used immediately, (2) limited *guidance* on *transfer impact assessments* and *risk mitigation measures,* (3) the non-operational nature of an independent supervisory agency with adequate *enforcement* powers, and (4) unclear mechanisms for data subjects to exercise their rights in the context of data transfer.

Harmonization with EU GDPR standards is a strategic necessity to strengthen Indonesia's position in the global digital economy ecosystem. Concrete recommendations include: first, the drafting of Indonesian SCCs that can be used directly by organizations; second, the development of comprehensive *guidance* on *transfer impact assessment* and *technical/organizational measures;* fourth, strengthening the capacity and independence of supervisory agencies with adequate *investigation* and *enforcement* powers; and fourth, improving the quality of *transparency* in digital platform *privacy policies* through clear templates and standards.

These harmonization efforts will not only strengthen the protection of data subjects' rights in the digital economy era, but will also increase Indonesia's competitiveness as an attractive destination for digital investment with a credible *regulatory framework* that is on par with international standards. Effective implementation of these recommendations will require strong collaboration between regulators, industry, and the public to ensure that personal data protection is not only *a compliance requirement* but also *a competitive advantage* in Indonesia's digital transformation.

Application of *Techno-Regulation* Theory in Developing an Accountable and Transparent Personal Data Transfer Mechanism Based on a Comparative Study of the EU GDPR as a Form of Personal Data Subject Protection in Indonesia

In the context of digital transformation, which is accelerating the transfer of personal data between data controllers, the urgency of developing accountable and transparent mechanisms has become a priority for the protection of personal data subjects' rights in Indonesia. The complexity of Indonesia's digital ecosystem, which recorded *e-commerce* transactions worth IDR 487 trillion in 2024 with 65 million active users, has created a layered personal data transfer flow that requires comprehensive and structured regulations (Sobandi, S., & Indriati, N. R., 2025). The *techno-regulation* theory developed by Lawrence Lessig provides a relevant conceptual framework for understanding how technology can be used as an effective regulatory instrument in protecting personal data, particularly in the context of data transfer between data controllers. This theory identifies four main points of regulation that influence individual behavior in cyberspace: *law*, social *norms*, *market*, and technological *architecture* (Lessig, L., 2000). In the context of personal data protection, technological architecture or "*code"* has regulatory capabilities equivalent to formal law because it can automatically restrict and regulate behavior through system design. This approach is highly relevant to the concepts of "*privacy*

by design" and "*privacy by default"* that have been adopted in the EU GDPR as fundamental principles in personal data protection (Rommetveit, K., & Van Dijk, N., 2022).

The implementation of *techno-regulation* theory in the context of personal data transfer requires harmonization between these four points to create a coherent and comprehensive regulatory ecosystem. Law as the first force provides a normative framework and sanctions, social norms create public expectations for privacy protection, the market provides economic incentives for *compliance*, and technological architecture ensures technical implementation in accordance with regulatory provisions. This comprehensive approach enables the establishment of personal data transfer mechanisms that not only fulfill formal legal aspects but are also responsive to technological dynamics and public expectations. The European Union has developed comprehensive best practices in regulating personal data transfers through the EU GDPR, particularly in Article 46, which regulates "*Transfers Subject to Appropriate Safeguards*." *The* EU GDPR *framework* provides a highly structured mechanism by providing a list of *appropriate safeguards* including SCCs, *binding corporate rules, approved codes of conduct,* and *approved certification mechanisms.* The advantage of the approach in the EU GDPR lies in the availability of approved SCC templates that can be used directly to facilitate data transfers with adequate protection for personal data subjects.

The implementation of the principle of transparency in the practice of personal data transfer in the European Union demonstrates a very comprehensive level of detail through the obligation of data controllers to provide very specific information to data subjects regarding every aspect of data processing and transfer. The information that must be provided includes the specific identity of the transfer recipient, the purpose and legal basis of the transfer, the risks that may arise, the duration of data storage, and the concrete procedures for exercising the rights of data subjects. This transparency is reinforced by the *DPIA* mechanism, which requires data controllers to conduct a comprehensive risk assessment before undertaking high-risk data transfers (Schrems, C. & Kuner, C., 2023). The principle of accountability in the EU GDPR is implemented through very strict obligations for data controllers to demonstrate their compliance with all regulatory provisions. This accountability mechanism includes complete documentation of the entire transfer process, implementation of DPIA for high-risk transfers, appointment of *a Data Protection Officer* for certain cases, obligation to report data *breaches* within 72 hours, implementation of periodic audits, and maintenance of comprehensive records of processing activities. A strong *enforcement* system is supported by *Data Protection Authorities* (DPA) that have investigative and law enforcement powers with significant administrative sanctions (van Laarhoven, E., 2023).

The absence of a Personal Data Protection Agency (LPDP) in Indonesia has created a significant functional authority vacuum in the prevention, supervision, and resolution of disputes over the transfer of personal data between data controllers. The PDP Law mandates the establishment of the LPDP as an independent authority in Articles 58 to 60, but as of mid-2025, this institution has not yet been formed, creating a legal loophole in personal data protection. The delay in establishing the LPDP has serious implications for the effectiveness of the implementation of the PDP Law, particularly in the context of personal data transfers that require systematic supervision and *enforcement*. The LPDP has a strategic role in preventing the failure of personal data protection through the authority mandated in Article 59 of the PDP Law, including the formulation and establishment of personal data protection policies, supervision of implementation, enforcement of compliance, and dispute resolution. In the context of personal data transfer between data controllers, the LPDP will play a crucial role in developing technical standards for data transfer, conducting compliance audits, and ensuring the implementation of the principles of transparency and accountability. The LPDP's functions also include the creation of templates and *operational guidance* that can be used directly by data controllers to facilitate transfers that are in line with the PDP Law.

A comparison with international best practices, namely the EU GDPR, shows that an independent supervisory agency with adequate capacity is a fundamental prerequisite for the effectiveness of personal data protection regulations. DPAs in the European Union have extensive powers to conduct investigations, audits, and law enforcement with the support of a strong organizational structure and guaranteed independence (Dimitrova, D., & De Hert, P., 2024). Indonesia needs an LPDP with similar characteristics to ensure that personal data transfers between data controllers can be carried out with adequate and consistent protection standards. EU GDPR SCCs are contractual instruments that have proven effective in ensuring secure personal data transfers that *comply* with high protection standards. EU GDPR SCCs have a modular structure that can be adapted to various transfer scenarios, equipped with detailed *annexes* describing the transfer, a list of parties and their respective roles, *categories of data subjects* and *personal data, sensitive data measures,* and *technical and organizational measures* (Marelli, M., 2024). Another advantage of SCCs is their *transfer impact assessment* mechanism, which requires parties to conduct a comprehensive assessment of the

specific circumstances of the transfer and implement appropriate risk mitigation measures (Greenleaf, G., 2022).

The adoption of SCCs in Indonesia by LPDP will provide significant benefits in the application of transparency principles because SCCs require data controllers to provide very detailed and specific information about every aspect of data transfer. The clauses in SCCs regulate in detail the identities and roles of the parties, the purpose and legal basis of the transfer, the categories of data transferred, the duration and method of transfer, and the rights and obligations of each party. This transparency is reinforced by the obligation to conduct complete documentation and periodic audits of the implementation of these clauses (Marelli, M., 2024). From an accountability perspective, SCCs provide a clear *framework* for demonstrating compliance with personal data protection provisions through systematic verification and audit mechanisms. SCCs require parties to implement adequate *technical and organizational measures*, conduct *regular assessments* of the effectiveness *of safeguards,* and provide audit access to supervisory authorities (Schrems, C. & Kuner, C., 2023). This mechanism enables the LPDP to effectively monitor and *enforce* data controller compliance in personal data transfers. The implementation of SCCs must also be accompanied by effective *remedy* mechanisms for personal data subjects whose rights are violated in the context of data transfers. The EU GDPR SCCs give data subjects the right to lodge *a complaint* with the DPA and obtain effective *judicial remedies*, including compensation for damages suffered. Indonesia needs to adopt a similar mechanism to ensure that personal data subjects have adequate access to legal remedies when violations occur in the data transfer process (Marelli, M., 2024).

The drafting of Indonesian SCCs must accommodate the specific characteristics of the legal system and national regulatory context while maintaining protection standards equivalent to those in the EU GDPR. Indonesian SCCs need to integrate the fundamental provisions of the PDP Law, particularly the rights of personal data subjects as stipulated in Articles 5 to 14, the principles of data processing in Article 16, and the obligations of data controllers in Articles 20 to 49. The structure of SCCs must be adapted to the types of data transfers that commonly occur in Indonesia, particularly transfers within the *e-commerce* ecosystem*, financial technology,* logistics service providers, and other digital services. The minimum content of Indonesian SCCs must include clauses regarding definitions and interpretations consistent with the terminology of the PDP Law, the obligations and responsibilities of the sending and receiving data controllers, *the technical and organizational measures* that must be implemented, *complaint handling* and personal data breach notification procedures, audit and monitoring mechanisms by the LPDP, the rights of personal data subjects and their implementation procedures, *sub-processing arrangements* and *chain of responsibility, data retention* and *deletion procedures, governing law* and *dispute resolution mechanisms,* as well as *termination procedures* and *post-termination obligations* (Schrems, C. & Kuner, C., 2023).

The Indonesian SCCs also need to accommodate the principle *of data minimization*, which requires that transfers only be made for personal data that is truly necessary for specific and legitimate purposes. This clause must be supplemented with verification and audit mechanisms to ensure that there is no *over-collection* or *beyond-purpose processing* in any transfer of personal data. The implementation of this principle requires *technical and organizational measures* that can ensure that only relevant and important data is transferred to the recipient (Cavoukian, A., 2009). The *enforcement* aspect of Indonesian SCCs must give clear authority to the LPDP to conduct investigations, audits, and enforce sanctions for violations of the agreed clauses. SCCs must include clauses that require the parties to provide full access to the LPDP in conducting supervision and audits, including access to documentation, systems, and personnel involved in the data transfer process. The sanction mechanism must be proportional to ensure optimal compliance from data controllers (DLA Piper., 2023).

The practical implementation of *techno-regulation* theory in the context of personal data transfer requires the integration of SCCs into the technology architecture through the concept of "*code is law*," which enables *automatic compliance* and *real-time monitoring* (Rommetveit, K., & van Dijk, N., 2022). *Technical measures* that can be implemented include *end-to-end encryption* in every data transfer, automated audit trails that record all transfer activities, *access control* that restricts access to authorized personnel only, and *data loss prevention systems* that prevent data transfers that do not comply with SCC provisions (Vázquez, J. L., & García-Sánchez, F., 2025). This technology architecture must be designed with the principle *of privacy by design* to ensure that personal data protection is integral to the organization's operational systems. The necessary *organizational measures* include appointing *a Data Protection Officer* responsible for implementing SCCs, conducting *regular training* for personnel involved in data transfer, implementing *incident response procedures* for *handling breaches* or *complaints,* and conducting *regular assessments* of the effectiveness of *the technical* and *organizational measures* that have been implemented (Cavoukian, A., 2009). This entire process must be comprehensively documented and accessible to LPDP for auditing and monitoring purposes.

Monitoring and *compliance checking* can be carried out through the implementation of *an automated compliance dashboard* that provides *real-time visibility* of all data transfer activities, *an automated alert system* for early detection of potential violations, *regular compliance reporting* to LPDP, and *third-party audits* by *certified auditors* to ensure the independence and objectivity of the assessment. This system must be designed with the capacity to integrate data from *multiple sources* and provide *a comprehensive view* of *compliance* (Jennifer Olomina, 2025). Harmonization with EU GDPR standards is a strategic necessity to strengthen Indonesia's position in the global digital economy ecosystem and facilitate data transfer between data controllers in Indonesia. The effective implementation of *techno-regulation* requires close cooperation between regulators, industry players, and the public. The goal is for personal data protection to be more than just a compliance obligation in fulfilling regulatory requirements, but also a competitive advantage in Indonesia's digital transformation. This approach will create a trustworthy and *sustainable* digital ecosystem with a level of personal data protection that is on par with international *best practices*, while still providing flexibility for innovation and digital economic growth in Indonesia.

CONCLUSION

A comparative analysis between Article 55 of the PDP Law and Article 46 of the EU GDPR shows that the regulatory framework for personal data transfers between controllers in Indonesia is still general and lacks technical details, creating legal uncertainty and the potential for data leaks or misuse. Article 55 of the PDP Law only stipulates general permission requirements without including security standards, verification procedures, or adequate documentation to ensure that the rights of data subjects are fulfilled throughout the transfer process. In addition, *the principles of transparency and accountability,* which include the obligation of controllers to provide detailed information regarding the identity of the recipient, the purpose of the transfer, the duration of storage, and audit measures, have not been regulated in concrete terms, ultimately reducing the effectiveness of protecting data subjects' rights in Indonesia.

To address these shortcomings, the first step that needs to be taken is the adoption of Indonesian SCCs. The government should develop SCC templates that integrate the rights of data subjects as stipulated in Articles 5–14 of the PDP Law and affirm the obligations of data controllers in accordance with Articles 20–49. This template must include minimum technical and organizational clauses, such as an appendix describing the transfer, a list of parties involved, categories of data transferred, risk mitigation measures, audit procedures, and a complaint resolution mechanism for data subjects. In addition, the clause must emphasize *the principle of data minimization* by limiting the type and amount of personal data to only what is relevant and proportional to the purpose of the transfer.

The second step is the establishment and strengthening of the Personal Data Protection Agency (LPDP) as an independent authority. The LPDP must have the authority to formulate technical standards for data transfer based on SCCs, issue guidelines for the implementation of DPIA, and conduct compliance audits. In order to be effective, the LPDP also needs to be given law enforcement powers in the form of investigations, administrative sanctions, and mechanisms for handling data subject complaints. The existence of the LPDP *is urgent* given the surge in e-commerce transactions that has triggered the volume of cross-platform personal data transfers, so that without a strong authority, the risk of data leaks and misuse will increase.

The third recommendation is to develop comprehensive guidance that includes DPIA guidelines and specific technical and organizational measures for high-risk data transfers. This guidance also needs to include a privacy notice template that contains detailed information about the data recipient, the purpose of the transfer, the legal basis, the storage duration, and the procedure for submitting subject rights, thereby increasing transparency and making it easier for data subjects to understand how their data is processed. This document must accommodate e-commerce best practices, including explicit consent mechanisms for the use of purchase data, consumer behavior tracking, and third-party integration.

Furthermore, the implementation of techno-regulation principles must be a focus, by applying compliance automation (*compliance by design*) such as *end-to-end* encryption, *automated audit trails*, access control systems, and *data loss prevention* so that data leaks can be minimized technically. In addition, the development of *real-time compliance dashboards* and *automated alert systems*, as well as the involvement of independent auditors, will provide continuous monitoring of data controller compliance, while ensuring that only minimal and relevant data is processed and transferred.

Finally, the implementation of effective *techno-regulation* requires close cooperation between regulators, industry players, and the public. The goal is for personal data protection to not only be a regulatory obligation, but also a competitive advantage in Indonesia's digital transformation. Ultimately, the active role of industry players and the public is no less important. Data controllers are required to

conduct regular training for personnel and appoint *a Data Protection Officer* (DPO) to ensure the implementation of data protection policies. Public campaigns and dialogue among stakeholders are necessary to foster a culture of transparency, accountability, and awareness of data subjects' rights in Indonesia's growing digital economy. Given the dynamics of the digital economy and the rapid growth of e-commerce, it is imperative for the government to finalize technical regulations and enforce oversight mechanisms to maintain consumer confidence and national competitiveness.

REFERENCES

Adhi Wicaksono. (2020, 06 May). 13 Juta Data Bocor Bukalapak Dijual di Forum Hacker. https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker

Agnes Z. (2025, 25 March). Nilai Transaksi E-Commerce Indonesia Capai Rp487 Triliun pada 2024. https://goodstats.id/article/nilai-transaksi-e-commerce-indonesia-capai-rp487-triliun-pada-2024-Vqv7l.

Amirudin. (2003). Pengantar Metode Penelitian Hukum, PT Raja Grafindo, Jakarta

Andanda, P., & Mlotshwa, L. (2024). Streamlining the ethical-legal governance of cross-border health data sharing during global health emergencies. Research Ethics, 20(4).

APJII. (2024, 07 February). APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang,

Ardika, I. W. C. (2025). Tinjauan hukum terhadap pelindungan data pribadi di era digital: Kasus kebocoran data pengguna layanan e-commerce. Indonesian Journal of Law and Justice, 2(3).

Bradford, L. (2021). Standard contractual clauses for cross-border transfers: a multi-layered risk-based approach. Journal of Data Protection & Privacy, 4(2).

Bradford, Laura, Mateo Aboy, and Kathleen Liddell. (2021) "Standard contractual clauses for cross-border transfers of health data after Schrems II." Journal of Law and the Biosciences 8, no. 1.

Cavoukian, A. (2009). Privacy by Design: The Seven Foundational Principles. Information and Privacy Commissioner of Ontario.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and data protection by design-from policy to engineering. arXiv preprint arXiv:1501.03726.

Dimitrova, D., & De Hert, P. (2024). DPA Independence and 'Indirect' Access—Illusory in Belgium, France and Germany? New Journal of European Criminal Law, 15(1).

DLA Piper. (2023). Indonesia: Personal Data Protection Law PDPL Now in Force.

Eberle, E. J. (2011). The methodology of comparative law. Roger Williams UL Rev., 16, 51.

Farhan Kalyara. (2024, 04 May). Data Pengguna Internet di Indonesia 2024 Meningkat Drastis. https://www.inilah.com/data-pengguna-internet-di-indonesia-2024.

Fernández, A.M. (2019). European Union · EDPB Opinion 14/2019 on Standard Contractual Clauses for Processors under Article 28(8) GDPR. European Data Protection Law Review.

Greenleaf, G. (2022). Transfer Impact Assessments Under the GDPR and the SCCs: Practical Guidance and Pitfalls. Computer Law & Security Review, 43, 105692.

Gumzej, N. (2023). DPA Powers toward Effective and Transparent GDPR Enforcement: The Case of Croatia. Tribuna Juridica.

Jennifer Olomina. (2025). AI-driven compliance monitoring frameworks for automated detection and classification of data privacy violations in hybrid infrastructures, International Journal of Science and Research Archive, 2025, 16(03).

Khaira Ummah Junaedi Putri. (2025, 17 April). Data e-commerce Indonesia: panduan lengkap", https://id.techinasia.com/data-ecommerce-indonesia-panduan-lengkap.

Leo Dwi Jamitko (2025, 23 January). Data APJII: Jumlah Pengguna Internet 2024 Tembus 225 Juta, Naik Tipis.https://teknologi.bisnis.com/read/20250123/101/1834155/data-apjii-jumlah-pengguna-internet-2024-tembus-225-juta-naik-tipis.

Lessig, L. (2000). Code and Other Laws of Cyberspace. Basic Books.

Lusa, S., Purbo, O. W., & Lestari, T. (2024). Peran e-Commerce dalam Mendukung Ekonomi Digital Indonesia. Penerbit Andi.

Marelli, M. (2024). Transferring Personal Data to International Organizations under Chapter V GDPR. International Data Privacy Law, 14(1).

Matthew, J., Rosadi, S. D., & Amalia, P. (2025). The User's Position as Personal Data Controller in the Utilization of Electronic Systems in the Form of Messaging Applications in Review of Law Number 27 of 2022 concerning Personal Data Protection. Journal of Law, Politic and Humanities, 5(4).

Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. Journal of cybersecurity and privacy, 4(3).

Murphy, M. H. (2022). Assessing the implications of schrems ii for EU–US data flow. International & Comparative Law Quarterly, 71(1).
Mutiara, U., & Maulana, R. (2020). pelindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas pelindungan Diri Pribadi. Indonesian Journal of Law and Policy Studies, 1(1).
Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. Cyber Security Dan Forensik Digital, 3(1)
Nathasya, S. N., Rosadi, S. D., & Pratama, G. G. (2024). COMPARATIVE STUDY OF PERSONAL DATA PROTECTION INDONESIAN CITIZENS IN TRANSBORDER PERSONAL DATA TRANSBORDER TRANSFER BETWEEN INDONESIA AND JAPAN. Syiah Kuala Law Journal, 8(1).
Phillip Lee (2021, 7 June). The updated standard contractual clauses — A new hope?. https://iapp.org/news/a/the-updated-standard-contractual-clauses-a-new-hope.
Pradana, M. A. E., & Saragih, H. (2024). Prinsip Akuntabilitas dalam Undang-Undang Pelindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya. Innovative: Journal Of Social Science Research, 4(4), 3412-3425
Putri, D. A., & Suryani, T. (2020). Analisis Dampak GDPR terhadap Manajemen Keamanan Data di Sektor Bisnis: Studi Kasus Indonesia. Kohesi: Jurnal Multidisiplin Saintek, 3(10).
Putri, N. M. D. G., Mahendrawati, N. L. M., & Ujianti, N. M. P. (2024). pelindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022. Jurnal Preferensi Hukum, 5(2), 240–245. https://doi.org/10.22225/jph.5.2.8087.240-245
Rahmawati, R., & Nurcahyani, N. (2024). ANALISIS PAJAK DIGITAL DI INDONESIA: KONTRIBUSI DAN TANTANGAN KE DEPAN. Jurnal Financia, 5(2)
Ramadhani, W. K. S., & Wiraguna, S. A. (2025). Implementasi pelindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan. Perspektif Administrasi Publik dan hukum, 2(2).
Rommetveit, K., & Van Dijk, N. (2022). Privacy engineering and the techno-regulatory imaginary. Social Studies of Science, 52(6).
Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.
Safir Makki. (2020, 31 October). Lazada Konfirmasi Perentasan 1,1 Juta Akun RedMart. https://www.cnnindonesia.com/teknologi/20201031103811-185-564335/lazada-konfirmasi-peretasan-11-juta-akun-redmart.
Schrems, C. & Kuner, C. (2023). Maximizing the GDPR Potential for Data Transfers. The Lancet Regional Health – Europe, 18, 100369.
Sobandi, S., & Indriati, N. R. (2025). Legal Gaps in Personal Data Protection and E-Commerce Responsibilities in Indonesia. International Journal of Law Reconstruction, 9(1).
Soerjono Soekanto. (2008). Pengantar Penelitian Hukum, UI Press, Jakarta
van Laarhoven, E. (2023). Accountability and Certification in the GDPR. SSRN Electronic Journal.
Vázquez, J. L., & García-Sánchez, F. (2025). Automating data transfer compliance and dispute resolution with smart contracts. Derecho e Innovación, 16(2).
Wright, A. & Goodwin, P. (2021). Data Subject Rights under the GDPR. Oxford University Press.