GHP law firm

Client Alert: Payment System Data Governance under Bank Indonesia Regulation No. 10 of 2026

I. Summary

On 29 October 2026, Bank Indonesia ("**BI**") issued Bank Indonesia Regulation No. 10 of 2026 on Payment System Data Governance ("**PBI 10/2026**"). The regulation establishes a framework governing the processing and exchange of payment system data, as well as the development and operation of Payment System Data Infrastructure (*Infrastruktur Data Sistem Pembayaran* or "**IDSP**").

PBI 10/2026 was introduced in response to the growing use of digital financial services and the resulting increase in payment transaction volumes, cybersecurity risks, and fraud. In line with the Indonesia Payment System Blueprint 2030, the regulation aims to strengthen risk management within the payment system industry and safeguard transaction integrity through more structured data governance and the establishment of the IDSP.

Pursuant to Article 4 of PBI 10/2026, the regulation applies to BI, Payment System Service Providers (*Penyelenggara Jasa Sistem Pembayaran* or "**PSPs**"), Connected Parties (*Pihak Terhubung*, i.e. parties authorized to connect with the IDSP), and other relevant parties. It also provides a basis for BI and relevant industry bodies to issue further technical requirements concerning payment system data processing.

II. Key Points

A. Data Governance and Processing Requirements

PBI 10/2026 introduces a more structured framework for the processing of payment system data, including data relating to individual and corporate users, as provided Under Article 8. Article 9 further provides that BI may classify user data into three categories: Public Data, Private Data, and Contractual Data, depending on the purpose and legal basis for its exchange.

Article 12 requires each Data Controller to ensure that user data is processed on a valid legal basis, including public task, legal obligation, vital interests, legitimate interests, consent, and/or contractual necessity. Under Article 11, BI may issue data governance policies on lawful processing, consent mechanisms, contractual standards, and data subject rights. If BI has not issued specific policies, PSPs must establish their own in accordance with applicable laws and requirements.

The regulation also requires data processing to be carried out in accordance with its intended purpose. Data processing under Article 22 of this regulation may involve three stages: data acquisition, data handling (including processing, storage, updating, and deletion), and data utilisation (including display, announcement, transfer, dissemination, and disclosure).

B. Fraud Management Obligations

Under Article 25, PSPs are required to establish and implement a comprehensive fraud management policy covering fraud prevention, detection, investigation and reporting, monitoring and evaluation, and education. This must be supported by appropriate risk management arrangements, including active oversight by their board of directors and board of commissioners, adequate policies and procedures, and clear organisational responsibilities.

Under Article 49, PSPs that are Connected Parties must examine payment transactions suspected of involving fraud as part of the IDSP's transaction integrity service. During the examination, they shall either temporarily delay the crediting of funds or refrain from

processing transactions to and from the recipient's account, including outgoing transfers, subject to the exceptions under the regulation.

Such measures may last up to five working days from the date of examination. PSPs must notify the relevant user in writing and, by the end of this period, determine whether to proceed with or reject the transaction based on the examination results. They must also maintain records of the examination, including relevant transaction details and the reasons for conducting it.

PSPs must also continuously monitor users recorded in transaction integrity data and apply appropriate customer due diligence and/or enhanced due diligence measures. They must not proceed with transactions involving such users, taking into account the user's latest status in the IDSP. Users may object to a decision not to proceed with their transaction, and PSPs must handle such objections in accordance with applicable consumer protection requirements.

C. Data Processing Impact Assessment

Article 28 requires PSPs and Connected Parties to conduct a data processing impact assessment before processing payment service user data. This assessment is intended to identify potential risks arising from the processing activity and determine appropriate mitigation measures, including measures to protect data subject rights.

The assessment must cover the nature of the processing, its necessity and purpose, potential risks, and corresponding mitigation measures. It will also serve as the basis for determining the feasibility, continuation, and risk control of the relevant data processing activities. Accordingly, PSPs and Connected Parties should incorporate this assessment into their data governance processes before commencing relevant processing activities.

D. Data Exchange and Contractual Requirements

PBI 10/2026 regulates the exchange of payment system data between BI, PSPs, and other relevant parties. Under Article 32, such exchanges may be conducted through or outside the IDSP.

For exchanges conducted through the IDSP, the parties are required to have an underlying document and designate a contact person. For exchanges outside the IDSP, PSPs are required to ensure that the relevant contractual arrangements contain minimum provisions addressing the purpose and scope of the exchange, the obligations of the sending and receiving parties, choice of law and dispute resolution, contract amendments and termination, data transfer procedures, and data subject rights and remedies. PSPs must also designate a point of contact for exchanges outside the IDSP.

Article 36 further provides that the underlying documents for data exchanges may include memoranda of understanding, connection agreements, and cooperation agreements. PSPs should therefore review their existing data-sharing arrangements to assess whether they meet the applicable requirements.

E. Payment System Data Infrastructure

Articles 41 and 42 provide for the establishment and administration of the IDSP by BI. The IDSP is intended to support, among other things, the unique identification of prospective and existing service users, the assessment of payment transaction integrity, and the exchange and storage of payment system data.

PSPs and other parties may apply to become Connected Parties and obtain access to the IDSP, subject to BI's approval and applicable requirements. These requirements under Article 45 include institutional criteria relating to legal entity status, financial condition, and management structure, as well as other requirements established by BI.

Connected Parties must comply with prudential principles, confidentiality, personal data protection requirements, applicable legal bases for data processing, information security standards, risk management requirements, and other requirements established by BI as stipulated in Article 46.

Parties providing data must ensure its accuracy and grant BI access to such data, while parties using data obtained through the IDSP must process it within the agreed scope and for the agreed purposes.

The PBI also sets out specific obligations for PSPs connected to the IDSP and requires reporting to BI upon request.

- User identification (Article 47): Connected PSPs must provide BI with data on prospective and existing service users and manage their unique identification.

- Transaction integrity data (Article 48): Connected PSPs must submit transaction integrity data through the IDSP, including data on users identified as involved in fraud. They must follow BI's rules on providing and using data, including obtaining consent where required and meeting applicable data standards.

- Ongoing monitoring (Article 50): Connected PSPs using the IDSP's transaction integrity service must closely monitor listed users, keep their information and transaction records up to date, and apply customer due diligence and/or enhanced due diligence, as applicable.

- Transaction refusals and objections (Articles 51–52): Connected PSPs must decline transactions by listed users based on their latest IDSP status and notify them in writing of the reasons and available next steps. Users may object to the refusal, and the relevant PSP must handle the objection in accordance with applicable consumer protection requirements.

- Reporting to BI (Article 64): PSPs and Connected Parties must report to BI, upon request, on their implementation of the payment system data rules, following BI's reporting procedures.

The IDSP and certain related obligations will be implemented in stages as determined by BI. Further requirements and implementation arrangements will be issued by BI. As part of the phased rollout, BI may require PSPs to become Connected Parties.

F. BI Supervisory Authority and Administrative Sanctions

PBI 10/2026 grants BI supervisory and monitoring authority over PSPs and Connected Parties in relation to compliance with the regulation and the implementation of the IDSP. BI may require relevant parties to take or cease certain actions, restrict activities, suspend data processing, or terminate access rights to the IDSP. BI may also publicly announce certain supervisory measures through its official website.

Administrative sanctions for certain violations may include written warnings, fines, temporary suspension of payment system data processing, temporary suspension of access to BI infrastructure, and other applicable administrative sanctions

III. Effective Date and Transitional Period

Under Article 76, PSPs must submit their fraud management policy and service-user data processing impact assessment to BI within one year of the regulation's effective date of 29 October 2026. PSPs designated by BI as first movers must submit their fraud management policy within three months of that date. PSPs must also submit any changes to either document to BI within 10 working days after the change is made.

IV. Practical Implications for Businesses

The In light of the new requirements, PSPs should consider taking the following steps:

1. **Review existing data governance policies and procedures:** Cover the required data processing activities have an appropriate legal basis, comply with applicable data protection requirements, and address relevant data subject rights.

2. **Assess and update fraud management policies:** Cover the required fraud management stages and establish procedures for examining suspected fraudulent transactions, including temporary transaction restrictions and user notification.

3. **Prepare data processing impact assessments:** Assess relevant data processing activities, identify potential risks, and establish appropriate mitigation measures before processing user data.

4. **Review existing data-sharing agreements:** Ensure that agreements contain the minimum contractual requirements under PBI 10/2026, including the purpose and scope of data exchange, parties' obligations, data transfer procedures, and data subject rights.

5. **Assess readiness to connect to IDSP as a Connected Party:** Assess eligibility and readiness to apply for connection to the IDSP, including institutional, operational, technological, and compliance requirements, and monitor further requirements issued by BI.

Further Information and Assistance

For more detailed advice or assistance, please contact our legal team:



Yosef Broztito
Partner
yosef.broztito@lawghp.com

GHP law firm

World Trade Center 3, Level 27
Jl. Jend. Sudirman Kav. 29-31
Jakarta 12920, Indonesia

T: +6221 50110199

www.lawghp.com

This publication has been prepared by GHP Law Firm for educational and informational purposes only. The information contained in this publication is not intended and should not be construed as a legal advice. Due to the rapidly changing nature of law, GHP Law Firm makes no warranty or guarantee concerning the accuracy or completeness of this content. You should consult with an attorney to review the current status of the law and how it applies to your circumstances before deciding to take any action.