ADP Counsellors at Law

THE BEST LEGAL SERVICE TO NAVIGATE YOUR BUSINESS

Insight

Payment ID: Between Innovation and Data Privacy Risk

Frenchelse Gorga Siahaan, S.H., M.H.

ADP Counsellors at Law
Plaza Simatupang 6th Floor Kav. IS No. 01, Jl. T.B. Simatupang, RT.2/RW.17, Pd. Pinang, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12310 | info@adplaws.com

Introduction

Bank Indonesia (BI) planned to launched the public trial of Payment ID on 17 August 2025, but later postponed it, because the need for technical improvement and better coordination between government institutions. Currently, Payment ID remains in the sandbox phase (a trial that used in the development of systems, technologies, and regulations) and one of that public trial is about the distribution of non-cash social assistance (bansos), that planned for September 2025 in collaboration with the local government in Banyuwangi.

Payment ID is a unique identification code based on the National Identification Number (NIK), designed to identify, record, and trace individuals' financial transactions in detail and it is part of the BI Payment Info development under the Indonesian Payment System Blueprint (BSPI) 2025–2030. Previously, Bank Indonesia launched BI-FAST as a real-time, efficient retail payment system. Payment ID now represents BI's effort to build a more integrated and transparent digital payment ecosystem.

Although BI assures that Payment ID will be used only with user consent and will not be accessed without the user's explicit authorization. As of now, there appears to be no publicly available technical regulation that serves as the system's primary legal framework. At present, the legal reference for Payment ID still falls under the broad provisions of Bank Indonesia Regulation No. 4/2025, which outlines high level payment system policies under the BSPI 2025–2030. However, this regulation functions primarily as a policy framework rather than a detailed operational guideline, leaving a regulatory gap regarding technical governance, data protection standards, and institutional accountability. In practice, therefore, the legal basis of Payment ID continues to rely on the general principles of Law No. 27 of 2022 on Personal Data Protection (PDP Law) and BI Regulation No. 4/2025, without any implementing regulations that address its practical operation. This leaves several critical aspects unregulated, including:

- Registration and verification mechanisms for Payment ID
- Procedures for deletion or modification of IDs by data subjects
- What legal consequences apply in cases of misuse or data breaches

Because Payment ID is directly linked to NIK, each digital transaction may, in principle, be traceable to an individual's identity. This design has prompted discussions on how to balance transparency and traceability with data protection and privacy safeguards. On the other hand, the system offers promising capabilities for detecting high-risk financial activities, including illegal gambling, unlicensed lending, and money laundering. Thus, the challenge lies not only in the technology itself, but in the extent to which the state can ensure that this innovation does not become a tool for violating on citizens' privacy.

Obligations Under Personal Data Protection Law

Given that Payment ID is based on NIK and records users' financial activity, it is likely to be classified as sensitive personal data under Article 4(2) of the PDP Law, depending on its usage context and the depth of data processing. Public discourse suggests that access to Payment ID data will be subject to user consent, in line with the general principles of the PDP Law. This aligns with Article 20(2), which requires explicit consent from data subjects for personal data processing.

However, challenges arise when data is used for investigative purposes or integrated with tax systems. Economist Acuviarta Kartabi, emphasizes that such integration must be request based and not automatic.

In the event of a data breach within the Payment ID system, primary responsibility lies with the Personal Data Controller, as defined under Law No. 27 of 2022. In the payment system context, entities that directly collect, store, and process user data such as Payment Service Providers (PJP) are typically classified as Data Controllers. Bank Indonesia, as the regulator and national payment system authority, primarily holds policy and supervisory responsibilities. Legal liability as a Data Controller would only arise if it were directly involved in the management or processing of personal data, as defined under the PDP Law., but does not automatically bear legal liability as a Data Controller unless it is proven to manage data directly.
Under the PDP Law, Data Controllers are obligated to:

- Safeguard data against unauthorized access, breaches, and misuse
- Notify data subjects in the event of a breach
- Provide recovery mechanisms and uphold user rights

If a data breach occurs due to negligence, such as inadequate security infrastructure or poor internal controls, Data Controllers may be subject to administrative or even criminal sanctions, depending on the gravity and consequences of the incident.

However, because the data governance structure for Payment ID has not yet been clearly regulated, there remains significant legal ambiguity regarding which entity would bear responsibility in the event of a breach. It is therefore imperative for the government to issue detailed technical regulations that clearly define the roles and responsibilities of each actor within the Payment ID ecosystem.

Conclusion

Bank Indonesia's decision to delay the launch of Payment ID reflects a cautious approach to ensuring technical and systemic readiness. However, despite the postponement, the urgency of derivative regulations remains critical, as each trial phase already involves the processing of citizens' personal data.

Payment ID is a significant innovation in Indonesia's national payment system. Yet, to prevent it from becoming a surveillance tool that infringes on privacy rights, the following safeguards are essential:

- Clear technical regulations governing implementation and oversight
- Transparent, user-friendly consent mechanisms
- Strengthening of independent oversight bodies to ensure data accountability
- Designation of responsible institutions in the event of data breaches

Without adequate legal safeguards, the implementation of Payment ID could inadvertently create risks of overreach that may conflict with fundamental principles of the rule of law and the protection of individual rights.

ADP Counsellors at Law

Office
Plaza Simatupang 6th Floor Kav. IS No. 01, Jl. T.B. Simatupang, RT.2/RW.17, Pd. Pinang, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12310

Email
info@adplaws.com

Tel.
+6221 2270 2291

ADP Counsellors at Law

THE BEST LEGAL SERVICE
TO NAVIGATE YOUR BUSINESS