

# Indonesia: The World's 4th Largest Population and a Key Market for Data-Footprint Businesses

Prepared by:

Mika Isac Kriyasa, Partner ([mika.kriyasa@dentons.com](mailto:mika.kriyasa@dentons.com)) and Steven Feriyanto (Associate)

With over 275 million people, Indonesia ranks as the fourth most populous country in the world, after China, India, and the United States. According to the World Bank and Indonesia's Central Bureau of Statistics (*Badan Pusat Statistik*), this number continues to grow at a steady rate, with a demographic that is overwhelmingly young, tech-savvy, and increasingly active online. This makes Indonesia one of the most promising markets globally for digital businesses—especially those reliant on data footprints, such as e-commerce platforms, financial technology companies, ride-hailing apps, health tech solutions, and digital advertising networks.

## A Digital Economy on the Rise

Indonesia's digital economy is booming. Google's e-Economy SEA 2022 report estimated that Indonesia's digital economy could reach US\$130 billion by 2025, driven by the rapid adoption of mobile internet and digital services. According to data from the Indonesian Internet Service Providers Association (APJII) and the Ministry of Communication and Information, Internet penetration in Indonesia was over 77% in 2023, with more than 210 million users online. Social media usage is among the highest in the world, and digital financial services are expanding rapidly, especially in underbanked areas.

All of this means one thing: data. Huge volumes of personal data are being collected, stored, processed, and analyzed every day—from shopping habits and travel patterns to health records and financial behavior. This massive and fast-growing data ecosystem has brought both economic opportunity and regulatory scrutiny.

## UU PDP: Indonesia's Landmark Data Protection Law

Recognizing the need to regulate this growing digital environment, Indonesia enacted its first comprehensive Personal Data Protection Law (*Undang-Undang Perlindungan Data Pribadi / UU PDP*) in 2022.

This law represents a major milestone in the development of Indonesia's digital legal framework and aligns the country more closely with global data protection standards, such as the European Union's General Data Protection Regulation (GDPR).

After a two-year transitional period, UU PDP became fully enforceable on October 17, 2024. The law provides clear rules regarding the collection, use, transfer, and storage of personal data. It defines the rights of data subjects (users) and the obligations of data controllers and processors (companies and institutions handling data).

## Key Provisions of Indonesia's Personal Data Protection Law (UU PDP)

Provision	Description and Article Reference
Effective Date	Fully enforceable starting October 17, 2024
Applies to	Indonesian and foreign entities processing personal data of people in Indonesia (Article 2)
Data Subject Rights	Access, correction, deletion, objection, and data portability (Article 5–15)

Provision	Description and Article Reference
Consent Requirement	Must be explicit, informed, and freely given (Article 20)
Data Breach Notification	Must notify authorities and users within 72 hours (Article 46)
Cross-Border Data Transfer	Permitted only under conditions with adequate safeguards (Article 56)
Administrative Sanctions	Written warnings, temporary suspension, deletion of data (Article 57–59)
Criminal Sanctions	Fines and imprisonment for serious violations such as unauthorized use or illegal sale (Article 67–73)
Data Protection Officer (DPO)	Required for high-risk data processing activities (Article 53)

### Extraterritorial Reach: Foreign Companies Take Note

One of the most significant aspects of UU PDP is its extraterritorial scope. The law applies not only to companies based in Indonesia, but also to any international company that processes personal data of Indonesian citizens or residents, regardless of whether the company has a physical presence in the country.

This means that if a foreign company offers services targeting the Indonesian market—such as through a website, mobile app, or marketing campaign—it is required to comply with UU PDP. This includes obtaining explicit consent from users, ensuring secure data processing, appointing a Data Protection Officer in some cases, and reporting data breaches within a specific timeframe.

### Obligations and Enforcement

UU PDP lays out a comprehensive set of responsibilities for data handlers, including:

- Obtaining informed consent before collecting or processing personal data;
- Providing transparency about how data will be used and for what purposes;

- Allowing individuals to access, correct, or delete their data;
- Ensuring data security through technical and organizational measures;
- Notifying regulators and users in the event of a data breach;
- Conducting cross-border data transfers only under permitted conditions.

The law also introduces administrative sanctions, such as fines and temporary suspension of business activities, as well as criminal penalties, including imprisonment for certain violations.

### Real-World Enforcement: Criminal Cases Already Emerging

Since the full enforcement of Indonesia’s Personal Data Protection Law (UU PDP) on October 17, 2024, the government has shown it is serious about protecting personal data. This is not merely a regulatory framework on paper—the law is already being actively enforced through criminal prosecutions.

Several early cases have made headlines. In one, a defendant used publicly available personal data to impersonate a police officer via WhatsApp and commit fraud (PN Karanganyar No. 5/Pid.Sus/2023/PN Krg). Two other cases from Tangerang (PN No. 77 and 78/Pid.Sus/2024/PN Tng) involved the unauthorized sale and commercial distribution of personal data. These cases reflect growing judicial recognition of digital privacy rights in Indonesia.

Several arrests have already been made, and prosecutions are underway under Articles 67 to 70 of the UU PDP, which provide for criminal sanctions, including imprisonment.

These developments send a strong signal to both local and international businesses: compliance with the UU PDP is not optional. Companies that target Indonesian consumers or operate within Indonesia’s jurisdiction must adhere to the law or risk criminal prosecution, substantial fines, and reputational damage.

### Opportunity Meets Responsibility

Despite the increased regulatory burden, businesses should see this shift as a positive one. A well-regulated data environment fosters trust, enhances transparency, and provides a clear framework for sustainable growth. Consumers are more likely to engage with brands that respect their privacy and protect their data.

For international companies, Indonesia represents an enormous market opportunity—but it also demands a proactive and compliant approach to data governance.

The earlier companies adapt their operations to align with UU PDP, the better positioned they'll be to succeed in this rapidly growing and digitally connected nation.

### Legal Support for Foreign Companies: Ensuring PDP Compliance in Indonesia

Dentons HPRP offers international companies tailored legal support to navigate and ensure compliance with Indonesia's Personal Data Protection Law (UU PDP). Key services include:

- **Adjusting Privacy Notices (Policies)** to ensure alignment with Indonesian legal requirements;
- **Reviewing Data Processing Activities** to assess risks and ensure compliance;
- **Preparing or reviewing legal bases for data processing**, such as explicit consent forms and data-related agreements;
- **Reviewing Internal Data Protection Policies**, including standard operating procedures and technical safeguards;
- **Assisting with Data Breach Incident Reports** to both the authorities and affected individuals;
- **Reviewing Data Breach Reports** for compliance with regulatory standards;
- **Drafting and/or reviewing agreements between controllers**, especially in joint ventures or shared platforms;
- **Drafting and/or reviewing agreements with data subjects**, including terms that meet Indonesian consent and disclosure requirements;
- **Drafting and/or reviewing processor agreements**, ensuring clear allocation of data protection responsibilities;

- **Providing legal opinions and solutions** in response to regulatory inquiries or business concerns relating to personal data protection;
- **Conducting Data Protection Impact Assessments (DPIAs) for high-risk processing activities**, as recommended under the UU PDP;
- **Training and Capacity Building for client teams on data protection compliance**, including workshops for in-house legal and IT staff;
- **Advising on Cross-Border Data Transfer Mechanisms**, including safeguards, adequacy decisions, and contractual clauses;
- **Regulatory Liaison Support**, including assisting clients in communicating with Indonesian data protection authorities;
- **Litigation and Enforcement Support**, including representation in administrative or criminal proceedings related to data protection breaches;
- **Monitoring Legal and Regulatory Developments**, providing clients with updates and guidance on emerging compliance obligations in Indonesia.

These services are essential for companies seeking to enter or expand in the Indonesian market while minimizing regulatory and reputational risk. Early engagement with experienced counsel can help businesses not only comply but also build consumer trust and long-term operational resilience.

\* \* \* \* \*

Indonesia's massive population, rapid digital growth, and evolving data protection framework make it a must-watch market for global businesses. However, thriving in this dynamic environment requires more than just offering a great product or service—it demands a strong understanding of Indonesian law, cultural context, and a firm commitment to compliance with local regulations such as the Personal Data Protection Law.

- o0o -

*The article above was prepared by Dentons HPRP's lawyers*

*This publication is not intended to be a comprehensive review of all developments in the law and practice, or to cover all aspects of those referred to. Readers should take legal advice before applying the information contained in this publication to specific issues or transactions or matters. For more information, please contact us at [dentons.hprp@dentons.com](mailto:dentons.hprp@dentons.com).*

*No part of this publication may be reproduced by any process whatsoever without prior written permission from Hanafiah Pongawa & Partners.*