Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Indonesia: Trends & Developments

Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur
ABNR Counsellors at Law

INDONESIA

Trends and Developments

Contributed by:
Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur
ABNR Counsellors at Law

ABNR Counsellors at Law was founded in 1967. It is Indonesia's longest-established law firm and has played a pivotal role in shaping the development of international commercial law in the country, particularly during its economic reopening to foreign investment in the 1960s. Today, with a team of around 120 legal professionals – including 27 partners and three foreign counsels – ABNR stands as Indonesia's largest independent, full-service law firm. The firm is proud to have female partners, reflecting its commitment to diversity and inclusion. ABNR has consistently maintained its position as a top-tier law firm since its establishment. As the exclusive Indonesian member of Lex Mundi since 1991 – the world's leading network of independent law firms with representation in over 100 countries – ABNR provides seamless global reach for its clients.

Authors

Agus Ahadi Deradjat (Agung) is a partner at ABNR and a former member of the firm's management board. Agung focuses his practice on corporate/M&A, foreign direct investment (FDI), and TMT. He advises leading domestic and multinational corporations across all leading industries and sectors, but offers particular expertise and experience in life sciences, technology and telecommunications, e-commerce and automotive. Agung has worked on a number of major M&A and FDI transactions for high-end multinational clients, as well as significant FDI transactions in the technology, pharma industry, manufacturing, chemicals, and the natural resources sectors. Agung is ranked for TMT (Band 1) and corporate and M&A by Chambers Asia-Pacific.

Mahiswara Timur joined ABNR as an associate in June 2015 and was made partner in January 2026. Timur focuses on IT-related assignments such as telecommunications networks (including for submarine cables and satellites) and services, cybersecurity, privacy and personal data protection, digital content compliance, cloud computing, e-commerce, broadcasting, over-the-top services, data centre operation, digital platforms and services in Indonesia, the internet of things, and online games. He has advised start-up clients and leading multinational technology, social media and streaming companies. His extensive understanding of the regulatory, technical and practical aspects of the TMT business has enabled Timur to provide precise, comprehensive advice as well as practical solutions well-tailored to client needs and business operations.

Nina Cornelia Santoso joined ABNR in April 2015 and became a senior associate in January 2022. Nina's main areas of professional practice encompass TMT, competition, M&A, and FDI. In TMT, she regularly advises high-profile multinationals and local companies on privacy and data protection, internet-based products and services (digital platforms, social media, online games, cloud computing, e-commerce, over-the-top services), cybersecurity, and content moderation. She occasionally advises clients on telecommunications networks and services matters (including subsea cables). Her graduate studies at the University of Cambridge provide her with a deep understanding of the EU General Data Protection Regulation (GDPR).

Contributed by: Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur,
ABNR Counsellors at Law

Dhan Partap Kaur (Sonia) is an associate at ABNR whose practice focuses on TMT, M&A, and general corporate law. In the TMT sector, Sonia regularly advises leading multinationals and local companies on data privacy and protection, internet-based services (digital platforms, social media, online games, cloud computing, e-commerce, and over-the-top services), cybersecurity, and content moderation. She is known for delivering tailored, practical solutions aligned with each client's business objectives and frequently provides hands-on support to clients navigating complex regulatory frameworks.

ABNR Counsellors at Law

Graha CIMB Niaga
24th Floor
Jl. Jenderal Sudirman Kav. 58
Jakarta
12190
Indonesia

Tel: +62 21 250 5125/5136
Fax: +62 21 250 5001
Email: info@abnrlaw.com
Web: www.abnrlaw.com

Contributed by: Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur,
ABNR Counsellors at Law

Indonesia's Evolving Data Protection Framework: Key Developments in AI, Cyber Resilience and Child Protection

PDP Law in a nutshell

Law No 27 of 2022 on Personal Data Protection (the "PDP Law") serves as the overarching law on personal data protection in Indonesia. In addition to the PDP Law, the implementation of personal data protection is subject to the following laws and regulations:

- the PDP Law;
- Law No 11 of 2008 on Electronic Information and Transactions, last amended by Law No 1 of 2024 (the "EIT Law");
- Government Regulation No 71 of 2019 on the Provision of Electronic Systems and Transactions ("GR 71/2019"); and
- other sector-specific regulations.

The PDP Law has extraterritorial effect, meaning that overseas organisations, including individuals, public entities, and international organisations, can be prosecuted in Indonesia for violating the law, particularly for non-compliance in processing personal data of Indonesian citizens, whether onshore or offshore. The Indonesian government has been working on the Draft Implementing Regulation for Law No 27 of 2022 on Personal Data Protection ("Draft GR PDP"), which is intended to provide further guidance on the law's implementation and enforcement. However, as of early 2026, there is no clear timeline for its finalisation. Based on the latest available public statement from the Ministry of Communications and Digital Affairs (MOCD) in October 2025, the Draft GR PDP has completed its harmonisation process, and has been passed to the State Secretary for approval by the President.

Furthermore, an amendment to the current PDP Law is currently included in the Annual Priority National Legislation Programme (which is prepared jointly by the House of Representatives, the Regional Representatives Board, and the President) for 2026. The amendment was registered on 23 September 2025 and is only at the planning stage.

Some of the notable provisions under the PDP Law are outlined below.

Types of personal data

The PDP Law defines "personal data" as "any data related to an individual (natural person), whether identified or capable of being identified independently or in combination with other information, whether directly or indirectly, through the use of an electronic system and/or non-electronic means". The individual is referred to as a "data subject".

The PDP Law further categorises personal data as general personal data (name, gender, nationality, religion, marital status, or personal data that together can identify a person) and specific personal data (data on health, biometric or genetic, and criminal records; data on children; financial data; and/or other data in accordance with the laws and regulations). There is no particular differentiation in treatment of the processing of general or specific personal data. However, the processing of specific personal data would trigger additional obligations, such as the need to perform a Data Protection Impact Assessment (DPIA) and appoint a Data Protection Officer (DPO).

Lawful basis for processing of personal data

The PDP Law acknowledges several legal bases for personal data processing: (i) consent; (ii) contractual necessity; (iii) compliance with a data controller's legal obligations; (iv) protection of the vital interests of the data subject; (v) public interest, for the provision of public services or for the exercise of lawful authority; and (vi) legitimate interest. We observe that the above legal bases are very similar to the concept adopted by the EU GDPR.

Cross-border data transfer

The PDP Law introduces layered requirements to allow data controllers to transfer personal data outside Indonesian territory, namely:

- (i) The country receiving the transfer of personal data has an equal or higher level of personal data protection than afforded under the PDP Law ("Adequacy of Protection").
- (ii) In the absence of Adequacy of Protection, an adequate level of binding personal data protection must be available ("Appropriate Safeguards").
- (iii) In the event that neither Adequacy of Protection nor Appropriate Safeguards are present, consent

for the cross-border data transfer must be given by the data subject.

Points (i) to (iii) above must be assessed and implemented in sequence. To date there is no indication that an official approved list of countries that meet the Adequacy of Protection requirements will be published.

Data Protection Authority (DPA)

The PDP Law mandates the formation of a DPA that is tasked to act as regulator, supervisor, and executor in data protection matters by the President, which is yet to be formed. In the meantime, pursuant to MOCD Regulation 1/2025 on Organisation and Work Procedures, matters concerning personal data protection are currently under the authority of Directorate General of Digital Space Supervision at the MOCD (DG). The DG is tasked with formulating and implementing policies related to digital space supervision and personal data protection. Based on statements made by the current Minister in public announcements, the DPA is expected to be established in the near future.

DPO

The PDP Law requires a data controller or data processor to appoint a DPO in situations where: (i) it processes personal data for public interest; (ii) the data controller's core activities have such a nature, scope, and/or purpose that require regular and systematic monitoring of personal data on a large scale; and (iii) the data controller's core activities involve large-scale processing of specific/sensitive or criminal-related personal data.

The Indonesian Constitutional Court, through Decision No 151/PUU-XXII/2024 dated 30 July 2025, held that this cumulative reading was unconstitutional. The word "and" the PDP Law must instead be read as "and/or," meaning that fulfilling any one of these conditions is sufficient to trigger the obligation to appoint a DPO. Thus, data controllers and data processors should reassess their obligations under the PDP Law to appoint a DPO.

Development on artificial intelligence (AI)

AI is increasingly being adopted across multiple sectors in Indonesia, including by government institutions in their daily operations. Recognising the growing demand for AI technologies, the government has indicated its support for AI development and is planning to accommodate its use through forthcoming regulations and infrastructure initiatives.

While Indonesia has yet to introduce binding regulations governing the use of AI, MOCD issued Circular Letter No 9 of 2023 on Ethics of Artificial Intelligence ("CL 9"). As of early 2026, CL 9 remains the only general regulatory guidance addressing the use of AI by business undertakings.

In summary, CL 9 contains the following salient items:

- general definitions, general guidelines for values, ethics, and control of consulting, analysis and programming activities with an AI basis by business undertakings and electronic systems operators (ESOs);
- emphasis that the CL 9 is applicable to: (i) business undertakings operating under Indonesian Standard Business Classification (KBLI, similar to ISIC) 62015 on AI-Based Programming Activities; (ii) ESOs in public scope; and (iii) ESOs in private scope; however, with the issuance of KBLI 2025 version, KBLI 62015 is no longer applicable (AI-based programming activity is now encompassed under several different KBLIs, which are the issuance of AI-based software under KBLI 58290 (Other Software Publication) and development of AI fundamental components under KBLI 62194 (Activities for Developing Fundamental Components of Artificial Intelligence)); and
- emphasis on ethical use of AI by adhering to the principles of inclusivity, humanity, safety, accessibility, transparency, credibility and accountability, personal data protection, sustainable development and environment, and protection of intellectual property.

Additionally, the Financial Services Authority (*Otoritas Jasa Keuangan,* or OJK) has issued a Code of Ethics for Responsible and Trustworthy AI in the Financial Technology Industry, which applies to financial technology providers. The Code also stipulates principles of AI utilisation in the financial services industry, which includes: beneficial, fair and accountable, transpar-

Contributed by: Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur,
ABNR Counsellors at Law

ent and explicable, and robust and secure principles. In the banking sector, the OJK has issued Artificial Intelligence Governance for Indonesian Banking, which provides guidance for Indonesian banks on the responsible development and deployment of AI and reiterates the application of these principles in banking activities.

In response to the increasing demand for AI-related regulations and infrastructures, the MOCD recently issued its Whitepaper Roadmap for AI ("AI Roadmap"), which includes the MOCD's intention to support the development of AI and ways to optimise AI as part of Indonesia's digital ecosystem development. The AI Roadmap includes the MOCD's five-year programmes and goals related to the development of AI, including the intention to conduct research on AI, create regulations and policies regarding the use of AI, building AI infrastructures, and conducting harmonisation and standardisation on the interoperability of AI systems used in ministries and institutions. The AI Roadmap also addresses personal data protection aspects in the development, uses, and operation of AI.

Update on cyber resilience

Pursuant to the Indonesian Cyber Security Landscape published by the National Cyber and Crypto Agency in 2024, there were 56,128,160 data exposures that affected 461 stakeholders in Indonesia. As of August 2025, the National Cyber and Crypto Agency (BSSN) recorded a total of 3.64 billion cyber-attacks. Recurring data breaches in Indonesia highlight vulnerabilities in the country's cybersecurity policies and systems, along with insufficient supervision and enforcement against perpetrators.

The current legal framework requires reporting data breaches to the MOCD and notifying data subjects, while cybersecurity incidents without a data breach must be reported to regulators and law enforcement. Below are the regulatory regimes for data breach and cybersecurity incident notification:

- PDP Law: Upon "failure to protect personal data", the data controller must notify both the affected data subject and the Data Protection Authority within 72 hours. This includes breaches that impact confidentiality, integrity, or availability of personal data, resulting in destruction, loss, alteration, or unauthorised access.
- Electronic System Operation Regulations (GR 71/2019): An ESO must: (i) report to relevant authorities and law enforcement if there is a serious system failure due to third-party interference, and (ii) notify data subjects if personal data protection fails within its system.

The BSSN has issued BSSN Regulation No 1 of 2024 on Cyber Incident Management ("BSSN Reg. 1/2024") in an effort to combat the high number of cyber incidents, establishing Cyber Incident Response Teams (CIRTs) at a national, sectoral, and organisational level. CIRTs are expected to manage cyber incidents through the following steps:

- handling of cyber incidents;
- mitigation and recovery from cyber incidents; and
- reporting and dissemination of cyber incident information.

The membership of the national CIRT consists of representatives from:

- the BSSN;
- ministries or institutions;
- state-run institutions owning and/or operating vital information infrastructure (IIV); and
- ESOs other than state-run institutions owning and/or operating IIV.

Ministries and institutions are also required to create their own sectoral CIRT, while stare-run institutions owning and/or operating IIV and ESOs other than state-run institutions owning and/or operating IIV are required to form an organisational CIRT.

The government is also preparing the Draft Regulation for Cyber Security and Resilience ("Cybersecurity Bill"), which is intended to strengthen national cybersecurity protection. This Bill will regulate information infrastructure providers, critical information infrastructure, and digital product/service providers to implement stricter cybersecurity standards by combining upstream (requirements), midstream (monitoring, evaluation, and assessment/reporting), and downstream (sanctions) approaches.

Based on the publicly available draft, the key points in the Cybersecurity Bill include the following:

- Relevant entities are encouraged to report cyber incidents within a certain timeframe, with a view to facilitating improvement and mitigation measures rather than imposing sanctions.
- It mandates the implementation of security standards throughout the digital product process to protect national infrastructure from cyber threats.

The Cybersecurity Bill is expected to be the legal basis for maintaining Indonesia's cybersecurity, sovereignty, and resilience amidst escalating global threats, complementing the existing EIT Law. On the House of Representatives' website, the Bill is only registered in the Medium-Term Annual Priority National Legislation Programme (2025-2029), and was last updated in November 2024. However, based on news articles in August 2025, the Bill is currently at the harmonisation stage, where the draft is deliberated among various ministries/agencies and relevant stakeholders.

Likely implementation of the Draft GR PDP

As noted above, the Indonesian government has been preparing the Draft GR PDP for some time. While it is expected to provide further guidance on the implementation of the PDP Law, the regulation has yet to be issued. In addition, the Draft GR PDP contemplates the conferral of certain regulatory powers on the DPA, which has not yet been established.

Some notable provisions under the Draft GR PDP (latest publicly available draft as of August 2023) are outlined below.

Requirements for reliance on lawful bases

The Draft GR PDP provides further guidance or requirements on reliance upon lawful bases of processing, including:

- Express Consent: If the data subject refuses to provide consent, the data controller cannot deny goods or services to the data subject, provided no personal data processing is involved. Additionally, the data controller must implement measures to identify users and ensure relevant personal data protection, including for services targeting children and individuals with disabilities.
- Contractual Necessity: In relying on contractual necessity, the agreement that serves as a basis for the personal data processing must: (i) obtain valid express consent from the data subject; (ii) fulfil relevant personal data protection measures; (iii) assess the risk impact on the data subject; (iv) balance interests between the data subject and controller; and (v) acknowledge the data subject's rights. If the data subject does not provide valid consent, the personal data processing is considered null and void.
- Legitimate Interest: This lawful basis can be relied upon if the data controller: (i) analyses the needs, objectives, and balance between the rights of data subjects and its own interests, demonstrating a legitimate interest in processing personal data, and (ii) assesses that processing for other legitimate interests does not harm or impact the data subject, ensuring steps are taken to reduce any potential impact.

Practical challenges arising from the existence of various lawful bases for data processing include the need for data controllers to appropriately identify the correct lawful basis for each processing activity. Given that the PDP Law lacks sufficient guidance, data controllers must exercise caution when identifying the purpose of data processing and selecting the appropriate lawful basis. This task requires careful assessment to ensure compliance with the law and to avoid potential risks associated with unlawful data processing. Therefore, it is advisable for data controllers to engage in continuous consultation with authorities or legal consultants to ensure proper understanding and implementation of the law, as well as to address any ambiguities or uncertainties related to the lawful bases for personal data processing.

AI technology providers and users must consider the use of personal data for AI learning, output creation, and feedback. The processing of personal data using AI must: (i) adhere to data protection principles under the PDP Law; (ii) rely on an appropriate lawful basis for processing; and (iii) implement safeguards throughout the processing stages. For instance, users of generative AI platforms must ensure they have secured the

necessary lawful basis, such as obtaining consent from individuals before processing their personal data on AI platforms.

Cross-border data transfer

As stated above, the PDP Law provides that a data controller may transfer personal data offshore should they fulfil the layered requirements of Adequacy of Protection, Appropriate Safeguards, or consent of the data subjects. Data controllers are expected to be fully responsible for implementing appropriate security measures in the processing of data transfer.

The Draft GR PDP determines the Adequacy of Protection for personal data transfers by assessing the recipient country's circumstances, including the existence of (i) personal data protection laws; (ii) a supervisory authority; and (iii) international commitments or obligations under legally binding conventions or resulting from participation in multilateral systems. The Data Protection Authority will compile the list of approved countries.

When using Appropriate Safeguards for transferring personal data abroad, the Draft GR PDP allows safeguards such as (i) agreements between the sender's and recipient's countries; (ii) standard contractual clauses; (iii) binding company regulations for a group; or (iv) other recognised instruments. Data controllers and processors must also meet additional obligations, such as recording the transfer cycle, mapping its implications, and ensuring that the transferred data is sufficient, relevant, and limited to the transfer's purpose.

In July 2025, the MOCD issued a press release on data transfer clauses in a Joint Statement on Framework for United States–Indonesia Agreement on Reciprocal Trade with the United States issued by the White House on 22 July 2025 ("Joint Statement") with the intention to remove the barrier in digital information trade. The Joint Statement stipulates that Indonesia will provide certainty regarding the ability to transfer personal data out of its territory to the United States. This statement raised concerns over the potential removal of barriers to cross-border personal data transfers, as this could undermine the level of personal data protection and appear inconsistent with the layered cross-border transfer requirements under the PDP Law. However, the MOCD assured that the Joint Statement is not a form of free transfer of personal data and that transfers will still be conducted based on Adequacy of Protection under Indonesian law. There is currently no further clarification on the implementation of such barrier removal for data transfers with the USA.

Online Child Protection Government Regulation

Government Regulation No 17 of 2025 on the Governance of Child Protection in the Operation of Electronic Systems focuses on mitigating the negative impacts of the digital space for children ("GR 17/2025"). Under GR 17/2025, "children" is defined as anyone under 18 years old.

GR 17/2025 outlines the responsibilities of ESOs in managing online products, services, or features, overseeing child protection governance in electronic systems, and enforcing administrative sanctions. It applies to ESOs that develop or operate internet-connected products, services, or features, such as websites, mobile apps, social media platforms, or gaming services.

Regarding children's personal data protection, GR 17/2025 addresses the following.

DPIA for children

ESOs must conduct a DPIA for any online product, service, or feature accessible to children before it is used by them. The DPIA should cover the processing activities, the provider's interests, the necessity and proportionality of the processing, a risk assessment for children's protection, and risk mitigation measures. Additionally, the ESO must maintain the DPIA documentation for as long as the product, service, or feature remains accessible to children, and include a plan to address identified risks before marketing the product.

Obligation to protect children's personal data

ESOs must provide clear information on minimum age requirements and implement technical and operational measures to ensure appropriate age verification for children using online products, services, or features, and establish reporting mechanisms to challenge or

adjust age verification decisions and address misuse of such online products, services, or features that violate or may violate children's rights. These measures should align with specified risks and protect children's personal data, secure electronic systems, and prevent unauthorised breaches. Data collected for age verification should only be used for that purpose and deleted once the age requirement is met. ESOs must also ensure that parental/guardian consent has been obtained for all processing of children's data. There are no exceptions to the requirement to obtain parental or guardian consent for the use of children's personal data.

Additionally, ESOs are prohibited from using children's personal data in ways that could harm their physical, mental, or overall well-being, and from developing products that encourage excessive data collection. Data should only be processed if necessary for the service, unless there is a strong reason in the child's best interest. Providers are also banned from using children's data for other purposes without justifiable cause. Lastly, ESOs must appoint a DPO to oversee compliance with child data protection laws and regulations.

The MOCD also passed MOCD Regulation No 9 of 2026 on 6 March 2026 on the Implementation of GR 17/2025. Through the MOCD Reg. 9/2026 press release, the MOCD stated that children under the age of 16 are no longer eligible to create accounts on high-risk platforms as of 28 March 2026. Implementation will be conducted in a gradual manner, starting with platforms such as YouTube, TikTok, Facebook, Instagram, Threads, X, Bigo Live, and Roblox.

Furthermore, there are additional key points as follows:

- Self-Assessment of Age Categories: ESOs are to conduct a mandatory self-assessment to ensure that the products, services, and features developed and/or operated by the ESO are in accordance with the minimum age limit of children and the applicable child age group classifications.
- Child Protection Design: ESOs are required to have and implement a child protection design to ensure that content accessible to children in the products, services, and features complies with the minimum age limit for children and the age group classifications of children and does not conflict with laws and regulations.
- Risk Profile Classification and Mitigation: MOCD Re. 9/2026 introduces the minimum indicators of risk profile categories, and ESOs' obligation to implement mitigation in relation to the risks.

Roles of DPOs in Indonesia

The PDP Law mandates that both data controllers and processors appoint an officer or staff member to oversee personal data protection functions and ensure compliance with regulations. Since the law's enactment, the number of DPOs in Indonesia has increased, along with the formation of DPO associations. To standardise DPO competencies, the Minister of Manpower issued Decree No 103 of 2023, setting National Competency Standards for Personal Data Protection. These standards guide authorities in developing qualifications, training, and certification for DPOs. However, there is no requirement to register DPOs with authorities.

The government is also actively making efforts to conduct occupational mapping in the information and communication technology field (which encompasses functional areas such as IT governance (including DPOs and Data Protection Executives)), digital product development, etc) through Decree of the Head of the Communication and Digital Human Resources Development Agency of MOCD No 8 of 2025 on the National Occupational Map, as amended by Decree No 45 of 2025. The decree details qualifications, scope of work, tasks and authorities, and is intended to ensure the equal spread of occupation in personal data protection in each functional area.

Suggested approach to establish compliance in Indonesia

Business undertakings should adopt a risk-based approach, which involves identifying, assessing, and managing potential risks associated with personal data processing. Rather than treating all risks equally, businesses should allocate resources to areas that present the greatest threat to data security and privacy, ensuring efforts are proportionate to the risks

Contributed by: Agus Ahadi Deradjat, Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur,
ABNR Counsellors at Law

involved. In doing so, organisations can prioritise the most critical compliance requirements effectively.

While there are currently fewer privacy-specific regulations on the use of AI, business undertakings in these sectors must still ensure compliance with the PDP Law. Business undertakings must also reassess their current cybersecurity measures in anticipation of the enactment of the Cybersecurity Bill, and ensure compliance with emerging child protection requirements in the digital space.

In light of the anticipated regulatory developments, business undertakings should closely monitor further updates to ensure timely awareness of any changes. This approach will allow business undertakings to take the necessary steps to anticipate any significant changes that may be introduced by the government from time to time. Early identification of material developments will allow sufficient time to implement the necessary compliance measures, thereby minimising operational risk and associated costs.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com