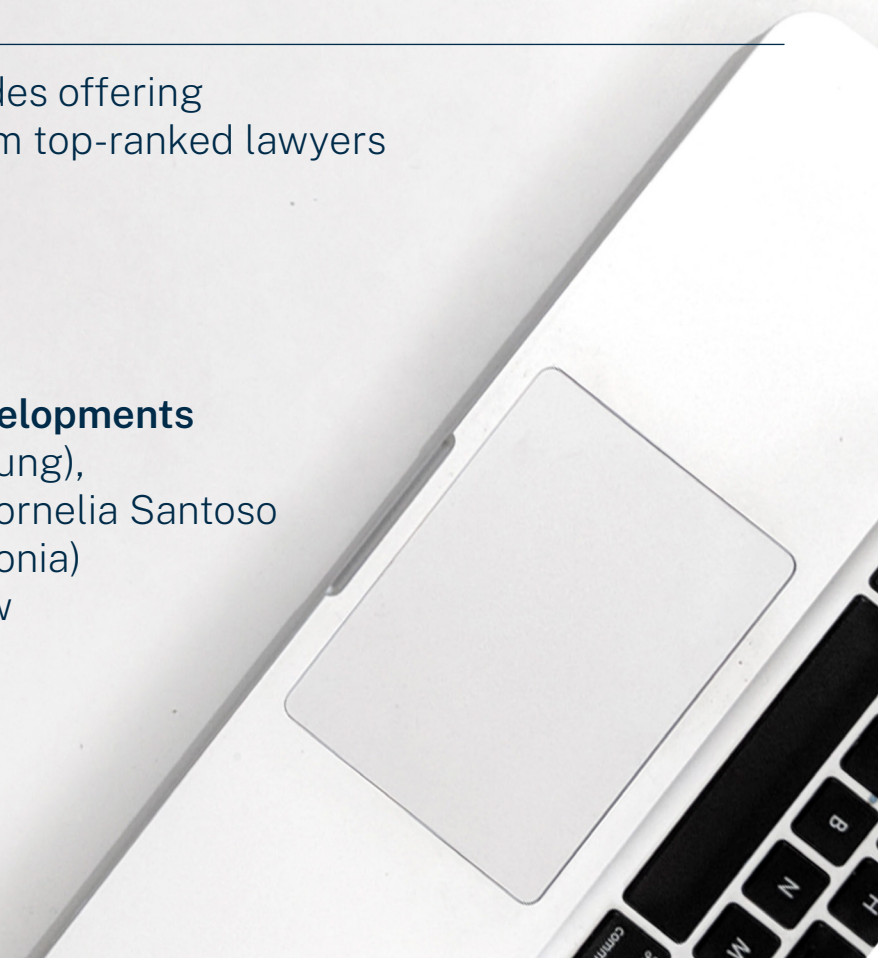
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2025

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



Indonesia: Trends & Developments

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

INDONESIA

Trends and Developments

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

ABNR Counsellors at Law was founded in 1967 and is Indonesia's oldest law firm. ABNR pioneered the development of international commercial law in the country following the reopening of its economy to foreign investment after a period of isolationism in the early 1960s. With more than 100 partners and lawyers (including two foreign counsels), ABNR is the largest independent full-service law firm in Indonesia and one of the country's top three law firms by number of fee earners, giving it the scale needed to simultaneously handle large and complex transnational deals across a range of practice areas. ABNR is ranked by Chambers and Partners as a Leading Firm in Chambers Asia-Pacific 2025 and Chambers FinTech 2025, and is also ranked in Chambers Global 2025.

Authors

Agus Ahadi Deradjat (Agung) is a partner at ABNR Counsellors at Law 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 recently 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 natural-resources sectors. Agung is ranked for TMT (Band 1) and Corporate/M&A in Chambers Asia-Pacific.

Mahiswara Timur joined ABNR Counsellors at Law as an associate in June 2015. Timur has focused 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-ups and leading multinational technology, social media and streaming companies. His extensive understanding of the regulatory, technical and practical aspects of TMT business has enabled him to provide precise, comprehensive advice as well as practical solutions well-tailored to client needs and business operations.

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

Nina Cornelia Santoso joined ABNR in April 2015 and became a senior associate in January 2022. Nina's main areas of professional practice encompass technology, media and telecommunications (TMT), competition, M&A, and foreign direct investment (FDI). In TMT, she regularly advises high-profile multi-national and local companies on privacy and data protection, internet-based products and services (digital platforms, social media, online games, cloud computing, e-commerce, and 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 contributed to her profound knowledge of the EU General Data Protection Regulation (GDPR).

Dhan Partap Kaur (Sonia) joined ABNR as an assistant lawyer in June 2015, and became an associate shortly afterwards. She graduated in 2015 from the Faculty of Law, Universitas Indonesia, majoring in Business and International Law. During her academic years, she was actively involved in university organisations and committees, especially the Asian Law Students' Association (ALSA). Prior to joining ABNR, she was an intern at a prominent law firm in Singapore, from which she gained valuable legal knowledge and experience. At ABNR, Sonia has been part of the teams of lawyers which handle projects relating to, among others, investment, labour, and general corporate matters.

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 (Agung), Mahiswara Timur, Nina Cornelia Santoso and Dhan Partap Kaur (Sonia), **ABNR Counsellors at Law**

Data Privacy Imperatives in Business: How Indonesia's PDP Law Has Evolved to Accommodate the AI, Healthcare and Financial Services Sectors

PDP Law in a nutshell

In 2022, the Indonesian Parliament passed Law No 27 of 2022 on Personal Data Protection ("PDP Law"), which is designed to serve as the overarching law on personal data protection. The PDP Law is largely modelled on the EU's General Data Protection Regulation (GDPR), regarded as the "gold standard" for personal data protection worldwide, thus demonstrating further effort by the Indonesian government to bring data protection into line with the industry standard.

In addition to the PDP Law, several existing laws and regulations related to personal data protection remain in force, provided that they do not conflict with the PDP Law. Accordingly, the implementation of personal data protection is subject to the following laws and regulations:

- PDP Law;
- Law No 11 of 2008 on Electronic Information and Transactions, last amended by Law No 1 of 2024 ("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 Law, which officially ended its two-year grace period, was enacted on 17 October 2024. Since then, 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 2025, there is no clear timeline for its finalisation.

Some of the notable provisions under the PDP Law include the following.

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).

Data controller and data processor

The PDP Law expressly differentiates between "data controller" and "data processor", which is a new concept under Indonesian laws. A data controller determines the purpose of, and controls, the personal data processing. A data pro-

cessor processes the personal data on behalf of the data controller. A data controller is fully accountable and liable to the data subject for the processing of their personal data. However, a data processor is only independently liable if it processes personal data in a manner that deviates from the data controller's instruction, order or purpose.

Lawful basis for processing of personal data

The PDP Law acknowledges several legal bases for personal data processing:

- consent;
- contractual necessity;
- compliance with a data controller's legal obligations;
- protection of the vital interests of the data subject;
- public interest, for the provision of public services or for the exercise of lawful authority; and
- legitimate interest.

The authors observe that the above legal bases are very similar to the concept adopted by the EU GDPR.

Rights of data subjects

The PDP Law acknowledges a data subject's right to obtain information, and the right to rectify, access, terminate processing (including to delete and/or destroy personal data), withdraw consent, object to automated decision-making, suspend or restrict processing, lodge a complaint and seek compensation, and data portability.

The PDP Law further mandates that data subjects' rights must not be implemented in an absolutist manner: they can be adjusted if considered prejudicial to certain interests (national defence and security, or to law enforcement, etc).

Cross-border data transfer

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

- (a) 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");
- (b) in the absence of Adequacy of Protection, an adequate level of binding personal data protection must be available ("Appropriate Safeguards"); and
- (c) 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 (a) to (c) 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

The PDP Law mandates the formation of a Data Protection Authority that is tasked to act as regulator, supervisor, and executor in data protection matters by the President. Whilst there have been efforts to expedite the establishment of the Data Protection Authority, this authority has yet to be formed. In the meantime, pursuant to Ministry of Communication and Digital Affairs (MOCD) Regulation 1/2025 on Organization and Work Procedures, matters concerning personal data protection are currently under the Directorate General of Digital Space Supervision's (DG) authority. The DG is tasked with formulating and implementing policies related to digital space

supervision and personal data protection. The current Minister of Communications and Digital stated through a news publication that the Data Protection Authority is intended to be established as soon as possible.

Development of the PDP Law implementation in sectoral regulations

Artificial intelligence (AI)

While there is no specific regulation on the use of AI at the moment, MOCD issued Circular Letter No 9 of 2023 on Ethics of Artificial Intelligence ("CL 9") on 19 December 2023 in an attempt to provide general guidance for business undertakings when utilising AI-based programs.

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 AI basis by business undertakings and electronic systems operators (ESOs);
- emphasis that CL 9 is applicable for:
  - (a) business undertakings operating under Indonesian Standard Business Classification (KBLI, similar to ISIC) 62015 on AI-Based Programming Activities;
  - (b) ESOs in public scope; and
  - (c) ESOs in private scope; 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* – 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, transparent and explicable, and robust and secure principles.

Healthcare

Healthcare in Indonesia has rapidly adopted technologies, including AI, especially during the COVID-19 pandemic. While there is no specific regulation for data protection in the healthcare sector, healthcare providers are still subject to the provisions of the PDP Law.

Minister of Health (MOH) Regulation No 24 of 2022 on Medical Records allows medical records to be stored digitally at healthcare facilities, including on servers and certified cloud computing. Healthcare facilities can collaborate with an ESO that has onshore data storage, provided the ESO obtains a recommendation from the relevant MOH department.

Financial services

With over two-thirds of the global population now engaged in financial services, there is growing concern over data security from both customers and regulators.

In response, the OJK has issued Regulation No 22 of 2023 on Consumer and Public Protection in the Financial Services Sector (POJK 22), which includes provisions on personal data protection. Many of the personal data protection provisions under POJK 22 align with those in the PDP Law, such as the following.

- POJK 22 requires Financial Services Providers (FSPs) to provide access to consumers to obtain a copy of their data and/or information. This is to comply with data subjects' access rights under the PDP Law.

- If an FSP transfers consumers' data and/or information offshore, they must fulfil the layered requirements, which are similar to those under the PDP Law, which also requires the FSP to ensure that the receiving country has adequate personal data protection.

However, as FSPs are subject to both the PDP Law and POJK 22, this creates a dilemma, as they could face sanctions under both regulations for the same conduct. This situation places undue pressure on FSPs and creates an unfair competitive disadvantage compared to businesses outside the financial services sector. Additionally, upon the issuance of other implementing regulations by both MOCD or OJK in the future, including the list of approved countries for data transfer, there may be duality of regulation.

Update on data breaches

Pursuant to the Indonesian Cyber Security Landscape published by the National Cyber and Crypto Agency, there have been 56,128,160 data exposures that affected 461 stakeholders in Indonesia. Recurring data breaches in Indonesia highlight vulnerabilities in the country's cybersecurity policies and systems, along with insufficient supervision and enforcement against perpetrators. Despite the existence of formal legal instruments on cybersecurity, cybersecurity awareness and comprehensive implementation of security measures, from a technical and organisational perspective, play an important role in anticipating and mitigating cybersecurity risks.

The Indonesian legal framework on data breaches requires reporting 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:
  (a) report to relevant authorities and law enforcement if there is a serious system failure due to third-party interference; and
  (b) notify data subjects if personal data protection fails within its system.

Likely implementation of the Draft GR PDP

As briefly touched upon above, the Indonesian government has been preparing the Draft GR PDP. This is expected to shed some light on general requirements under the PDP Law, although the draft also confers some authority on the Data Protection Authority (which has yet to be formed) to regulate certain matters.

Some notable provisions under the Draft GR PDP include the following.

Requirements for reliance on lawful bases

Data controllers may rely upon other appropriate lawful bases such as contractual necessity, legal obligations, or vital, public, or legitimate interest.

The Draft GR PDP provides further guidance and requirements on reliance upon the lawful bases, including as follows.

- 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 of the personal data processing must:
  (a) obtain valid express consent from the data subject;
  (b) fulfil relevant personal data protection measures;
  (c) assess the risk impact on the data subject;
  (d) balance interests between the data subject and controller; and
  (e) 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:
  (a) 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
  (b) 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 is still relatively new and 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:

- adhere to data protection principles under the PDP Law;
- rely on an appropriate lawful basis for processing; and
- 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.

Definition of children

The PDP Law classifies data on minors as a special category but does not define "children" within the context of personal data. Definitions vary across regulations: the Indonesian Civil Code defines a child as someone under 21 and unmarried, while Law No 23 of 2002, amended by Law No 35 of 2014, defines a child as someone under 18. The Draft GR PDP clarifies this by defining a child as anyone under 18 and unmarried.

Under the PDP Law, there are no exceptions to the requirement of obtaining parental or guard-

ian consent for the use of minors' personal data, including for financial services, healthcare, or AI software for education and entertainment. Service providers must ensure that (i) parental or guardian consent is obtained for any services used by minors, and (ii) the person authorising the service is indeed the parent or legal guardian.

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, and consent of the data subjects.

Data controllers are expected to be fully responsible for implementing appropriate security measures in the processing of data transfer. Particularly, in the financial services sector, the POJK 22 mainly governs cross-border transfer of customers' information.

- For the transfer of individual customers' information, the FSP must comply with personal data protection laws and regulations, including those that are determined by the OJK. In this case, according to the PDP Law, the transfer of individuals' personal data must be based on:
  (a) Adequacy of Protection;
  (b) Appropriate Safeguards; and
  (c) the data subject having provided their consent.
- For the transfer of corporate customers' information, the FSP must be based on:
  (a) Adequacy of Protection as determined by the OJK;
  (b) Appropriate Safeguards deemed as acceptable by the OJK, for which POJK 22 provides further details on what would constitute Appropriate Safeguards, such as bilateral agreement, binding corporate rules, and standard contractual clauses determined by the OJK; and
  (c) securing consent from the customer.

The Draft GR PDP determines the Adequacy of Protection for personal data transfers by assessing the recipient country's circumstances, including:

- the existence of personal data protection laws;
- a supervisory authority; and
- international commitments or obligations from legally binding conventions or 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:

- agreements between the sender's and recipient's countries;
- standard contractual clauses;
- binding company regulations for a group; or
- 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.

Following the enactment of the PDP Law and the absence of Draft GR PDP, businesses and industry associations have taken proactive steps to ensure compliance with the existing legal requirements. The Indonesian Data Protection Practitioners Association (*Asosiasi Praktisi Per-*

lindungan Data Indonesia or APPDI), for example, has started developing compliance toolkits and Records of Processing Activities (RoPA) templates to help organisations manage and document their data processing activities in line with the intended regulations. These initiatives aim to provide clarity and guidance during the interim period while awaiting the finalisation of the Draft GR PDP.

Draft Online Child Protection Government Regulation: addressing personal data protection for children

The MOCD has also prepared a draft regulation that focuses on mitigating the negative impacts of the digital space for children ("Draft GR Online Child Protection"). This regulation, once enacted, will be a derivative of the EIT Law and the PDP Law.

The Draft GR Online Child Protection regulation 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. The Draft GR Online Child Protection regulation does not provide exemptions for financial services, healthcare, or AI software for education and entertainment that may be targeted towards child users.

Regarding children's personal data protection, the Draft GR Online Child Protection regulation 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 implement technical and operational measures to ensure appropriate age verification for children using online products, services, or features. 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. Providers must also offer mechanisms for users to challenge or adjust age verification decisions and report privacy or security violations, ensuring accessibility and fairness without unjustly restricting children's access to services.

Additionally, ESOs are prohibited from using children's personal data in ways that could harm their physical, mental, or overall wellbeing, 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 dedicated officer or staff to oversee compliance with child data protection laws and regulations.

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. Based on industry practices and the authors' observations, privacy professionals and practitioners are often referring to standards and certifications from the International Association of Privacy Professionals (IAPP), considering the IAPP is offering comprehensive privacy certifications based on various jurisdictions' privacy regulations, including the GDPR which is similar to the Indonesian PDP Law.

Suggested approach to establish compliance in Indonesia

In order to establish compliance with data protection laws 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 involved. In doing so, organisations can prioritise the most critical compliance requirements effectively.

Furthermore, business undertakings in the fields within financial services must assess risk with higher scrutiny as the sector of financial services is highly regulated. While there are less privacy-specific regulations on healthcare and the use of AI, business undertakings in these sectors still must ensure compliance with the PDP Law.

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