Client Update: Indonesia
1 December 2022

A Practical Guide to Getting Your Organisation PDP Law-Ready

As a follow-up to our last client update (click here to read the client update) on the personal data protection framework in Indonesia, the personal data protection bill was finally numbered as Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**") and came into effect on 17 October 2022.

Given the wide-reaching implications of the PDP Law on businesses, we have set out key facts about the PDP Law, as well as a compliance checklist below. We hope that this checklist can be a useful starting point for you in examining your data protection policies to ensure compliance with the new data protection framework in Indonesia.

Key Facts

- The PDP Law grants a **two-year transitional period** from 17 October 2022 for data controllers, data processors, and other parties related to a data processing activity to adjust their data processing practices with the PDP Law's requirements.

- However, based on our informal discussions with the relevant Indonesian government officials, some provisions of the PDP Law became **effective immediately** from 17 October 2022. These are the provisions on **prohibited conducts related to data processing activities**, which are considered as criminal offences.

- The PDP Law **does not apply retroactively** to data processing activities carried out before 17 October 2022.

- **Administrative sanctions** under the PDP Law range from written warning, temporary termination of personal data processing activities, deletion or destruction of personal data,

and/or administrative fine. In addition, **imprisonment, criminal fine, asset confiscation, asset freezing, license revocation, and business dissolution (among many others)** may also apply.

- The PDP Law will apply to **businesses based both inside and outside of Indonesia**. For further details on the application of the PDP Law to your businesses, please read our previous client update.

Compliance Checklist

This checklist gives a general overview of the key requirements of the PDP Law. Besides describing the relevant key provisions of the PDP Law, it details the actions that businesses should take to ensure compliance with the PDP Law.

Please note that this checklist is based on best market practice and is by no means exhaustive. We encourage clients to reach out to their counsels for further advice.

No.	Reference to the PDP Law and Description	Recommended Actions
1.	**Lawful Basis for Processing Personal Data (Articles 20 and 21)**	
	First, you should identify the applicable lawful basis for processing personal data before you commence any such processing. The PDP Law regulates six lawful bases for personal data processing. The basis that is most appropriate for you will depend on the purpose for processing and your relationship with the data subject. In summary, the six lawful bases are: (a) explicit consent; (b) contractual obligation; (c) legal obligation; (d) vital interests; (e) public interest; and	You should: ☐ examine the various types of data processing that you carry out; ☐ identify the lawful bases that apply to you; and ☐ internally and externally document the processing activities (e.g., internally in your records of processing activity/data inventory and externally in your privacy notice). If you are relying on explicit consent as your lawful basis for processing personal data, you should review **how** you request consent from the data subject. The PDP Law sets a high standard for consent in that there must be a genuine choice (e.g., it cannot be a precondition of service and separate from other terms and conditions) and control over how you use the data subject's data.

No.	Reference to the PDP Law and Description	Recommended Actions
	(f) legitimate interest.	If your current practice on obtaining consent does not meet the PDP Law's high standards or is poorly documented, you need to seek fresh PDP Law-compliant consent, identify a different lawful basis for your processing, or stop the processing.
2.	**Data Subject's Rights**	
	(a) **Right to be informed (Article 5)** Your business must provide privacy information to data subjects.	If you already have a privacy notice, you should ensure that such notice complies with the PDP Law, including: ☐ that it contains the minimum required information (e.g., lawful bases used, purposes of processing, and data subjects' rights); ☐ that it is easy to understand and easy to access; and ☐ that it must be written in clear and plain language, including making available the Indonesian language text.
	(b) **Right to rectification (Article 6)** Your business must allow data subjects to correct and update their personal data.	You should: ☐ introduce appropriate systems to rectify or complete information, or allow data subjects to give supplementary statements, including to respond to data subjects' request for rectification within the prescribed period (3 x 24 hours); ☐ have procedures to inform the potential rectification with other organisations with whom you have shared personal data; and

No.	Reference to the PDP Law and Description	Recommended Actions
		☐ conduct regular data quality review of your systems and manual records to ensure the information in such systems and records continues to be adequate for the purposes of processing (for which it was collected).
(c)	**Right to access (Article 7)** Your business must provide data subjects the right to request access to their personal data.	You should: ☐ ensure that you have a process in place that allows you to recognise and respond to any requests for personal data within the prescribed period (i.e., 3 x 24 hours); and ☐ provide awareness training to all staff and specialist training to individuals who deal with such a request.
(d)	**Right to erasure (Article 8)** Your business must have a process to securely dispose of personal data that, among others, is no longer required or is subject to a deletion request from the data subject.	You should: ☐ have a procedure in place that allows data subjects to request the deletion or erasure of their information within the prescribed period (i.e., 3 x 24 hours) in your possession if, among other things, there is no compelling reason for you to continue processing such an information; ☐ have a procedure to inform the request for erasure with other organisations with whom you have shared the foregoing information with; ☐ have a procedure to delete information from any back-up systems; and ☐ implement a written retention policy or schedule to remind you when to dispose of various categories of data, and help you plan for its secure disposal.

No.	Reference to the PDP Law and Description	Recommended Actions
(e)	**Right to withdraw consent (Article 9)** Your business must give data subjects the right to withdraw their consent at any time.	You should: ☐ have a procedure in place that allows data subjects to request the withdrawal of their consent; and respond to such request within the prescribed period (3 x 24 hours); and ☐ consider using a privacy dashboard or other tools.
(f)	**Right to object to automated decision-making, including profiling (Article 10)** Your business must give data subjects the right to object to the processing of their personal data. The PDP Law protects data by allowing them not to be subject to a decision if such a decision is based solely on automated processing, including profiling.	You should: ☐ introduce a process for data subjects to obtain an explanation of the decision and request a review; and ☐ implement procedures and safeguards to address the risks involved with this type of processing.
(g)	**Right to restrict processing (Article 11)** Your business must give data subjects the right to request a restriction on the processing of their personal data.	You should: ☐ implement a process that enables data subjects to submit a request to you; ☐ have a process to act on a data subject's request to block or restrict the processing of their personal data; within the prescribed period (i.e., 3 x 24 hours); and ☐ if possible, have a procedure to inform about the request of restriction with other organisations with whom you have shared the foregoing information with.

No.	Reference to the PDP Law and Description	Recommended Actions
	(h) **Right to data portability (Article 13)** Your business must give data subjects the right to move, copy, or transfer their personal data from one IT environment to another.	You should: ☐ keep every personal data in a structured, commonly used, and machine-readable format, such that upon request from a data subject, such data subject's data can be easily moved, copied, and transferred; and ☐ have a process to allow you to recognise and respond to any data subject's request in line with your legal obligations and the statutory timeline (i.e., 3 x 24 hours).
3.	**Data Protection Impact Assessment ("DPIA") (Article 34)**	
	Your business must conduct a DPIA if you are planning to conduct data processing that has a high risk on the data subject's rights/interests.	You should: ☐ establish a policy setting out on when you should conduct a DPIA, who will authorise it, and how it will be incorporated into the overall project plan; ☐ assign responsibility for completing DPIAs to a staff who has sufficient control over the project to effect change; ☐ where a DPIA is required, ensure you complete the process before starting the project; and ☐ ensure that your DPIA process includes consultation with the DPO/data protection lead or other relevant stakeholders.

No.	Reference to the PDP Law and Description	Recommended Actions
4.	**Data Security (Article 35)**	
	Your business must put the appropriate security safeguards in place.	You should: ☐ assess the risks to the personal data in your possession and determine the level of security that is right for you; ☐ based on the above assessment, establish and implement a robust information security policy, which details your approach to information security, the technical and organisational measures that you will be implementing, and the roles and responsibilities staff have in relation to keeping information secure; ☐ implement periodical checks for compliance with the above policy, to give assurances that security controls are operational and effective; and ☐ deliver regular staff training on all areas within the information security policy.
5.	**Breach Notification (Article 46)**	
	Your business must notify the affected data subjects and the data protection authority of any personal data breaches.	You should: ☐ train staff how to recognise and report breaches; and ☐ have a process to report breaches to the appropriate individuals and data protection authority as soon as staff become aware of them, and to investigate and implement recovery plans.

No.	Reference to the PDP Law and Description	Recommended Actions
6.	**Accountability (Article 47)**	
	Your business must be able to demonstrate **how** it complies with the PDP Law's requirements.	You should: ☐ establish and implement a data protection policy that clearly sets out your approach to data protection together with responsibilities for implementing the policy and monitoring compliance. ☐ This policy will help you address data protection in a consistent manner and demonstrate accountability under the PDP Law; and ☐ The management should approve the policy and you should publish and communicate it to all staff. You should review and update the policy at planned intervals or when required to ensure it remains relevant.
7.	**Data Protection Officers ("DPO") (Article 35)**	
	Your business may need to appoint a DPO if you: (a) are processing personal data for public services (e.g., public authority); (b) carry out a large-scale regular and systematic monitoring of data subjects as part of your core activity (e.g., online behaviour tracking); and[1] (c) carry out a large-scale processing of specific personal data or data relating to	You should: ☐ assess if you are required to appoint a DPO, and if so, designate the responsibility for data protection compliance to a suitable individual, as well as allocate budget and prepare organisational structure; ☐ support the appointed individual by giving the appropriate training; and

[1] The PDP Law indeed states "and" in relation to the DPO appointment requirements. This means a controller/processor that is subject to such requirements must meet all the three prescribed conditions. However, we believe this was not the drafter's intention and it was merely a case of bad legislative drafting. Based on general best practice (e.g., the European Union's General Data Protection Regulation), the three conditions do not need to be fulfilled cumulatively, but instead alternatively (meaning a controller/processor only needs to meet one condition in order for the DPO appointment requirements to apply).

No.	Reference to the PDP Law and Description	Recommended Actions
	criminal convictions and offenses as part of your core activity.	☐ ensure there are appropriate reporting mechanisms in place between the above individual and the management.
8.	**Cross-Border Data Transfer (Article 56)**	
	Your business may only transfer personal data outside of Indonesia if you comply with the conditions for transfer set out in the PDP Law: (a) the jurisdiction where the recipient is located must have an equivalent or higher data protection standard; (b) the data exporter puts in place the appropriate and binding safeguards; or (c) in the absence of (a) and (b) above, the data exporter can proceed on the basis of the data subject's consent.	You should: ☐ ensure that any data you transfer outside of Indonesia complies with the conditions for transfer set out in the PDP Law; and ☐ ensure that you have adequate safeguards and data security in place, that is documented in writing (e.g., a contract).

Conclusion

As mentioned earlier, during the two-year transitional period, majority of the provisions in the PDP Law will not be immediately implemented. It is likely to be the case that the government will enact implementing regulations to the PDP Law, including on the establishment of the data protection authority.

However, it does not mean that businesses should adopt a "wait and see" approach until the end of the transitional period or the enactment of the implementing regulations. Rather, businesses should start proactively complying, especially considering that some of the provisions of the PDP Law are already effective. Businesses can refer to the general best practice in the market, whether in Indonesia or overseas, and can use the above compliance checklist as a starting point

Contacts

Zacky Zainal Husein
Partner

D +62 21 2555 9956
F +62 21 2555 7899
zacky.husein@ahp.id

Muhammad Iqsan Sirie
Partner

D +62 21 2555 7805
F +62 21 2555 7899
iqsan.sirie@ahp.id

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

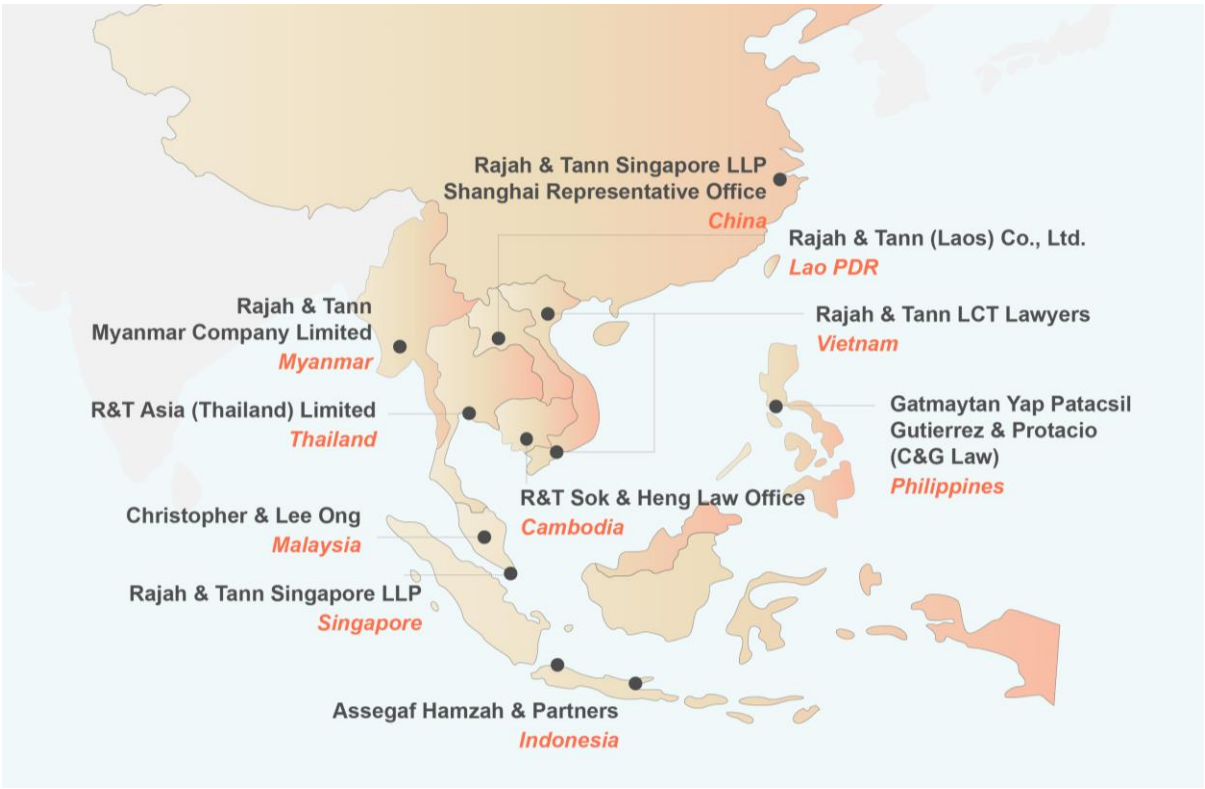
Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Client Update: Indonesia

1 December 2022

Our Regional Presence



Based in Indonesia, and consistently gaining recognition from independent observers, Assegaf Hamzah & Partners has established itself as a major force locally and regionally and is ranked as a top-tier firm in many practice areas. Founded in 2001, it has a reputation for providing advice of the highest quality to a wide variety of blue-chip corporate clients, high net worth individuals, and government institutions.

Assegaf Hamzah & Partners is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.