Linklaters Widyawan & Partners

Indonesia passes its long-awaited data protection bill: Key implications for your business

September 2022

On 20 September 2022, Indonesia's House of Representatives finally passed into law the long-awaited Data Protection Bill.

The Data Protection Law ("**Law**") marks a new era for the privacy law regime in South East Asia's most populous market, as the first overarching regulation on data protection. Indeed, the Law comes at a right time, amidst various high-profile data breaches in Indonesia that have recently put data management in the headlines.

Although passed by the House of Representatives, an official copy of Law is yet to be published, pending signature by Indonesia's President within 30 days of the House's decision. The final Law is therefore expected to be published and enacted by mid-October 2022.

What requires attention?

Based on the approved draft, the Law introduces several key principles and requirements:

Scope – Unlike existing regulations on personal data protection, which only cover personal data that is processed through an electronic system, the Law protects any personal data that are processed either through electronic systems or non-electronic systems. The Law also acts as an overarching regulation applicable to various sectors. Until now, data protection regulations in Indonesia have been provided across separate sectoral regulations, making navigation potentially difficult for businesses in an ever-convergent digital world.

Roles and responsibilities – The Law differentiates between data controllers and data processors. In general, a data controller is subject to more robust requirements compared to a data processor. A data processor is also only able to process personal data based on the instruction of the data controller. Data controllers can be any natural person, corporation, public agency, or international organization, acting independently or jointly in determining the purposes and exercising control over personal data processing.

Personal data – Personal data is differentiated under the Law into two main categories, ie (i) specific personal data (eg health information, criminal records, personal finance information, etc.), and (ii) general personal data (eg name, nationality, religion, marital status, etc.). While, in general, both specific and general personal data are subject to the same requirements under the Law, similar to the approach under the EU's GDPR, specific personal data is subject to certain additional requirements, eg impact assessment on processing of specific personal data by data controller.

Processing conditions – The Law reiterates earlier rules' bases for processing personal data, most of which are familiar to other GDPR-modelled regimes, ie (i) explicit consent of the data subject to the purpose(s) of the personal data processing disclosed to him or her, (ii) fulfilment of a contractual obligation in favour of the data subject who is a party to the agreement or as requested by the data subject at the time of entering into an agreement, (iii) fulfilment of legal obligations of the data controller in accordance with applicable laws and regulations, (iv) fulfilment of the vital interest of the data subject, (v) implementation of duties for the purpose of public interest, public service and/or implementation of data controller's authority pursuant to applicable laws and regulations, and/or (vi) fulfilment of another legitimate interest, in consideration of the purpose and interest of the data controller and the data subject's rights.

Consent mechanism – While previously any consent for collection, use or other processing of personal data must be made in writing, the Law now gives businesses more flexibility by allowing such consent to be evidenced by (audio) recording.

Cross-border transfer of personal data – Unlike existing rules which require the exporter of personal data to file a notification with the Minister of Communications and Informatics ("**MOCI**") before and after transfer, the Law requires no such notification (including on the designated jurisdiction); instead, it allows a data controller to transfer personal data to another data controller or data processor outside of Indonesia, provided that the jurisdiction in which the personal data is received has at least an equivalent standard of personal data protection as provided under the Law. The Law contemplates that further provisions on cross-border data transfers will be issued under an implementing regulation. Crucially, it remains to be seen which markets are deemed to be "adequate" to use the GDPR terminology. The Law, however, indicates that the data protection institution has the power to conduct assessment on fulfilment of the requirements for cross border personal data transfer. It is not clear whether the assessment would be done as part of the notification before transfer – we expect this would be clarified in the implementing regulations.

Data breach notifications – If there is a data breach or other failure to protect data, the data controller must notify the relevant data subject within 72 hours, as well as the relevant government institutions (as is the case under the GDPR for regulator notifications). This is a stricter requirement than that under the currently applicable IT regulations, for which the deadline to notify the data subject is 14 days after becoming aware of such breach.

M&A transaction – A legal entity data controller that is subject to a merger, consolidation, acquisition, spin-off or liquidation must notify the relevant data subjects before and after the corporate action. This is rather intriguing provision given that transfer of personal data must be based on explicit consent of the personal data subject. This provision will be further elaborated on in a government regulation; therefore, it remains to be seen – as in some other jurisdictions – whether this provision works as an exemption to the requirement to obtain data subject consent. In the meantime, transaction parties may need to take a risk-based view on how to approach disclosure of transactions.

Data protection officer – Data protection officers are chiefly responsible for ensuring their appointing entity's compliance with the applicable data protection laws and regulations. A data controller or data processor must appoint a DPO if it handles personal data processing for the public interest, the core activity of data processing requires structured and systematic supervision over large volumes of data, the core activity of data processing relates to processing of large volumes specific personal data and/or personal data relating to criminal activities. No thresholds are yet prescribed to determine what amounts to large-scale processing in this context.

Data protection institution – The Law contemplates that the President will establish a data protection institution, which will be responsible for (among others) supervising compliance with data protection requirements, imposing administrative sanctions and facilitating alternative dispute resolution for data protection cases. At this stage, there has been no further update on the plan and progress of this establishment.

Retention period – There is no specific retention period, therefore, technically the 5-year retention period set out in the MOCI Regulation No. 20 of 2016 concerning personal data protection in electronic systems should still be valid for personal data processed through electronic systems. Further guidance on this point is awaited.

Transitional provision – Any data controller, data processor and other parties involved in personal data processing are obliged to make necessary adjustments to comply with the provisions of the Law within 2 years from the date on which it is enacted. Businesses will welcome this grace period but it will be important that implementing rules are released in good time to allow proper adjustments to be made.

Sanctions – The Law provides additional and more severe sanctions for regulatory breaches, including criminal sanctions, specific actions (e.g. seizure of proceeds from the criminal actions), as well as sanctions for corporations (such as suspension of business activities). Whereas enforcement action has been generally been low in Indonesia under existing laws, this is expected to change with enactment of the Law.

Implementing rules

The Law also contemplates issuance of at least 10 further implementing regulations. At this stage though, it does not appear that the Indonesian government has started the preparation process. There will be certain aspects of the Law that can only be implemented or enforced following issuance of the implementing regulations and establishment of the data protection institution, eg an objection procedure for data subjects, further implementation of data subjects' rights, rules for data protection officers and the framework for operation of the data protection institution.

It also remains to be seen how the Law might impact the requirements currently provided under the various data protection regulations currently in force, such as the retention period (as explained above) and the requirements for exporting personal data (ie, the pre-notice and post-report obligations to MOCI). Interaction between authorities which have divergent mandates has been known to slow the implementation of data laws in other Asian markets.

Next steps

Before signature by the President, revisions to the Law are possible under the Indonesian legislative process. In practice, however, we would expect any last changes to be mostly redactional. We will provide a further update when this important piece of legislation is published, but are happy to start brainstorming implementation strategies with businesses operating in and with the Indonesian market.

Key contacts

Yolanda Hutapea
Partner, Jakarta
Tel: +62 21 2995 1596
yolanda.hutapea@linklaters.com

Teguh Arwiko
Partner, Jakarta
Tel: +62 21 2995 1554
teguh.arwiko@linklaters.com

Alex Roberts
Counsel, Shanghai
Tel: +86 21 2891 1842
alex.roberts@linklaters.com

Kevin Eduard Matindas
Associate, Jakarta
Tel: +62 21 2995 1513
kevin.matindas@linklaters.com