UNSW Law & Justice Research Series

Indonesia Enacts Personal Data Protection Act, With a DPA

Andin Aditya Rahman
and Graham Greenleaf

[2022] *UNSWLRS* 49
(2022) 178 *Privacy Laws & Business International Report* 22-24

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

INDONESIA ENACTS PERSONAL DATA PROTECTION ACT, WITH A DPA

Andin Aditya Rahman and Graham Greenleaf[**]

(2022) 178 *Privacy Laws & Business International Report* 22-24

[**] Andin Aditya Rahman is an Associate at Assegaf Hamzah & Partners. This article expresses his personal views and does not necessarily reflect the opinion of his firm. Email: andin.rahman@ahp.co.id ; Graham Greenleaf is Professor of Law & Information Systems, UNSW, Sydney

Electronic copy available at: https://ssrn.com/abstract=4343593

After introducing its first comprehensive draft bill on personal data protection in early 2016,[1] the Indonesian parliament considered various drafts, including one without a data protection authority (DPA). The Parliament finally passed the personal data protection bill into law on 20 September 2022, leaving India, Pakistan, and Bangladesh in the Asian region as the only significant countries without comprehensive data protection legislation.

The Bill contains a total of 16 chapters and 76 articles, including provisions on the types of data that are under the scope of the Bill, rights of data subjects, data processing by data controllers and processors, obligations of data controllers and mandatory appointment of data protection officers (DPO), the data protection authority (DPA), and administrative and criminal sanctions for non-compliance.

The Bill is accompanied by an Elucidation which provides some explanation to many articles. It will also be supplemented by Rules and Regulations for many specified provisions.

Scope: General and specific data

Before the PDP Bill, personal data protection under Indonesian law was mainly governed under its technology and cyberspace laws, which only apply to electronic personal data. With the enactment of the PDP Bill, provisions on personal data protection will also apply to non-electronic personal data.

The Bill classifies data into specific personal data, and general personal data (art. 4). Specific personal data shall include : (i) health information, (ii) biometric data, (iii) genetic data, (iv) criminal records, child data and (v) personal financial data, and 'other data in accordance with provisions of laws and regulations' (art. 4(2)). 'General data' includes among others: (i) complete name, (ii) gender, (iii) citizenship, (iv) religion, (v) marital status, and (vi) other forms of data that can identify a certain person if combined (art. 4(3)). This final clause appears to bring 'general data' into line with most data privacy laws internationally, by making 'identifiability' the key element of the definition of 'personal data'.

The Bill's scope is comprehensive: it covers individuals, corporations, public agencies and international organisations that are processing personal data.

The Bill has extra-territorial scope. In addition to applying to processing by parties located within Indonesia, it also applies to processing outside the jurisdiction of Indonesia 'which has legal consequences within Indonesia, or for Indonesian data subjects and citizens outside the jurisdiction of Indonesia (art. 2(1)).

Controllers and Processors

Responsibility for data processing by data controllers and by processors is specified. Data controllers are parties that determine the underlying purposes for the processing of the data of data subjects and simultaneously have control over the processing of the data.

In processing data, data controllers may engage with data processors that process the data on behalf of the controllers, in which the controllers will be held responsible for the processing of data conducted by the data processor and the data processor must carry out the processing of data in accordance with the instructions from the data controller that appointed them.

Rights of Data Subjects

[1] Andin Aditya Rahman '"Indonesia introduces a comprehensive privacy Bill"' *Privacy Laws & Business International Report*, February 2016.

Electronic copy available at: https://ssrn.com/abstract=4343593

. In contrast with the previous versions of the Bill, the Bill now uses the term data subjects instead of data owners, which broadens the scope of persons entitled to enjoy the rights under the Bill.

The rights of data subjects under the Bill include (arts. 5-15):

1. Request information relating to identity, the legal basis of processing, purpose of processing, as well the accountability of any party that requests data from the data subject;
2. Complete, renew, and amend mistakes or inaccuracies relating to their data;
3. Access and obtain copies of their data;
4. Have their data destroyed or data processing terminated;
5. Withdraw consent that they have granted to any data controller in relation to their data;
6. Object to any act or any decision-making processes that is based on automatic processing, including profiling (such processing should be based on a government Regulation);
7. Postpone or limit the processing of their data on a proportional basis;
8. File a civil lawsuit and receive indemnities (compensation) in relation to any violation of their data (this will also be based on a government Regulation);
9. Obtain or utilize their data provided by the data controller in a commonly recognized form or format; and
10. Submit their data to other data controllers provided that the relevant systems are capable of safely communicating with each other (data portability).

The above rights may be waived ('are excluded') based on reasons of: (i) national defence and security interests, (ii) law enforcement processes, (iii) the public interest as it relates to the organization of the state, (iv) supervision of the financial services sector, monetary and payment systems and the overall stability of the financial system, and (v) statistical and scientific research (art. 15).

Principles Required for Data Processing

In terms of data from data subjects, data controllers and processors may process data subject to the provisions under the Bill. The Bill asserts that data processing includes: (i) processing and analysis, (ii) storage, (iii) correction and renewal, (iv) display, announcement, transfer, dissemination, or disclosure, (v) erasure or destruction, and (vi) acquisition and collection of data.

In engaging in any data processing, data controllers and processors must adhere to the following principles (art. 16(2):

1. Limited and specific: processing of data must be carried out in a limited and specific manner, as well as legally and in a transparent manner;
2. Purpose: data processing must be carried out in accordance with the originally stated purpose;
3. Subjects' rights: data processing must ensure the relevant data subjects' rights;
4. Accuracy: data processing must be carried out accurately, comprehensively, and in a way that is not misleading, must be up to date, and may be held accountable;
5. Protection: data processing must be carried out in a way that protects data security and protects the data from illicit access, disclosure, alteration, misuse, damage, and/or removal;
6. Information: data processing must be carried out by informing the relevant data subjects of the purposes and activities that underlie the data processing, as well as any occurrences of data protection failures;
7. Erasure: data must be terminated and erased after the retention period has passed, or based on the request of the data subject, except otherwise stipulated by law; and
8. Responsibility: data processing should be carried out responsibly and provide for clear accountability.

In addition to the above, the Bill also affirms (art. 17) that data processing devices or visual data processors (commonly referred to as closed-circuit television or CCTV), where they operate in public places and/or public service facilities, must be operated in accordance with the following:

Electronic copy available at: https://ssrn.com/abstract=4343593

1. For the purpose of security, disaster prevention, and/or traffic management or traffic information collection, analysis and regulation;
2. Must display Information in areas where visual data processing or processing devices have been installed; and
3. Not used to identify a person.

Legitimate Basis For Personal Data Processing

A personal data processor must have a legitimate basis for processing personal data (art. 20). Data processing can be conducted legitimately based on:

1. Explicitly valid consent granted by the data subject in question for one or multiple certain purposes that the data subject has been informed of by the data controller;
2. Contractual obligations: if data subjects are contracting parties or in order to fulfil the data subjects' requests when formulating agreements;
3. Legal obligations of a data controller in accordance with prevailing laws and regulations;
4. Data subject's vital interests relating to the data subject's mortality (for example, if it is required in relation to serious medical condition of the data subject);
5. Public interest, public services or the implementation of the data controller's authorities based on laws and regulations, such as administration of residency data; and
6. Other valid interests, including debt collection, legal prosecution, and employee supervision, taking into account the interests of the controller and the data subject.

There are special provisions for processing children's data (art. 25), and persons with disabilities (art. 26).

Data Protection Officer (DPO)

In processing data, data controllers and processors must appoint a DPO if: (i) the processing of data is carried out for public service interests, (ii) the data controller's core activities fulfil the criteria of activities that require periodic and systematic monitoring of large-scale data, or (iii) the data controller's core activities entail large-scale processing of specific data, or relate to data concerning criminal offences.

The Bill does not further elaborate the above criteria for data controllers and processors to be subject to the requirement to appoint a DPO. It is expected that this will be further detailed in an implementing regulation of the Bill.

Data Protection Authority (DPA)

The DPA under the Bill is primarily in charge of overseeing compliance and imposing administrative sanctions for non-compliance. However, the Bill has opted to establish its DPA under the President (art. 58(3)), and making the DPA 'responsible to the President' (art. 58(4)). The Bill mandates the president as well as the government to issue the regulation for its establishment and to further detail the DPA's functions and authorities (art. 58). However, the Bill itself sets out many particular obligations and authorities that the DPA will have (arts. 59-60).

This places its independence under scrutiny, because an independent institution under Indonesian law is established by legislation (not by the president or government). This puts into question any form of enforcement by the DPA, considering that the DPA has been mandated by the Bill to also oversee government authorities in terms of data protection.

'The settlement of a Personal Data Protection dispute shall be conducted through arbitration, court, or other alternative dispute resolution agencies in accordance with provisions of laws and regulations' (art. 64).

Electronic copy available at: https://ssrn.com/abstract=4343593

Sanctions for Non-Compliance

Any non-compliance with the Bill will be subject to administrative sanctions by the DPA, which may include written warnings, temporary suspension of data processing activities, erasing or destroying the relevant data, mandatory compensation, or administrative fines. Administrative fines may be as high as 2% of the annual revenue of the Controller concerned. Breaches subject to such administrative fines are defined (art. 57).

In terms of criminal actions, the Bill addresses four activities that are classified as such (arts. 67-73). These criminal actions include: (i) unlawful obtaining and collection of data (maximum five-year imprisonment and/or maximum fine of IDR 5 billion), (ii) unlawful disclosure of data (maximum four-year imprisonment and/or maximum fine of IDR 2 billion), (iii) unlawful utilization of data (maximum five-year term of imprisonment and/or maximum fine of IDR 5 billion), and (iv) falsification of data (maximum six-year of imprisonment and/or maximum fine of IDR 6 billion). One billion Indonesian rupiah is worth approximately USD $64,000.

In addition to the above sanctions, the Bill provides additional criminal sanctions that may also be imposed, including confiscation of profits, assets, or proceeds from the criminal actions, and compensation payment.

If the criminal action is conducted by a corporation, the criminal sanctions are rendered to the management, controller, or beneficial owner of the corporation, and the criminal fine for corporations can be imposed up to ten times the maximum of the criminal fine for individuals. Corporations may also be subject to the imposition of additional sanctions in the form of: (i) confiscation of profits and/or assets obtained, or proceeds generated from the criminal act, (ii) total or partial suspension of the corporation's business, (iii) permanent prohibition on engaging in certain activities, (iv) total or partial shutdown of the corporation's place of business or activities, (v) requirement to fulfil the neglected obligations, (vi) payment of compensation, (vii) revocation of relevant licenses, and/or (viii) dissolution of the corporation (see in particular arts. 72-73).

Compensation

Data Subjects have the right to sue in the courts and receive compensation for violations of the processing of their personal data, 'in accordance with provisions of laws and regulations' (art. 12(1)). Further provisions concerning compensation shall be in a Regulation of the Government (art. 12(2)). This will be a government-wide regulation, not one of a specific agency.

International Transfers and Cooperation

Transfer of personal data by a data controller in Indonesia to a data controllers outside Indonesia is regulated by a number of steps:

(i) The Indonesian data controller must ensure that the country of domicile of the controller or processor that receives the transfer of Personal Data 'has a Personal Data Protection level that is equal to or higher than those that are regulated under this Law' (art. 56(2));

(ii) Otherwise, the Indonesian controller 'must ensure that there is adequate and binding Personal Data Protection.' (art. 56(3)).

(iii) Otherwise the Indonesian controller must obtain approval of the personal data subject (in Indonesia) (art. 56(4)).

The government can also make a Regulation governing this area (art 56(5)).

International cooperation between the government and other governments on data protection matters is authorised (art. 63).

Electronic copy available at: https://ssrn.com/abstract=4343593

Conclusions and comparisons

Looking forward, Indonesia may have set its foot on the road of data protection by enacting the Bill, but the direction of the step that it will take remains to be seen, if the Indonesian DPA is not provided with proper independence to uphold what remains of the Indonesian data integrity. Nevertheless, the Bill (now an Act) is Indonesia's comprehensive data privacy legislation that was previously lacking and (at best) scattered throughout various sectoral laws. Those laws have managed – up to a point – to place emphasis on ensuring compliance by corporations through stipulating specific sanctions for corporations.

Having already been approved by the DPR (Parliament), the PDP Bill is currently awaiting the president's signature in order for it to be designated a number and be passed into law. However, the PDP Bill will automatically enter into force if the president does not sign it within 30 days of it being passed by the DPR (the last date was on 20 October 2022).

Looking at the PDP Bill from the perspective of the whole of Asia, there are quite a few aspects that could be emulated: it is a 'comprehensive' Bill, not one which is 'private sector only (contrast Singapore, Malaysia and perhaps Brunei; it has a separate Data Protection Authority, though one where there is room for argument about how independent it will be. The possibility that administrative fines may be as high as 2% of the annual revenue of the Controller sets a precedent for such fines in other South-East Asia and South Asia countries. The provisions for compensation are yet to be finalised through Regulations, but at least the Act does include them.

Compared with the current benchmark for data privacy laws, the EU's General Data Protection Regulation (GDPR), many other 'modern' aspects are included (at least in theory) in Indonesia's law, such as explicit protection of genetic and biometric data as sensitive data; withdrawal of consent to processing; limits on automated decision-making; 'proportionality' as a factor limiting processing; 'data portability'; requirement of a basis for personal data processing; requirements for personal data protection impact assessments in specified settings; and appointment of Data Protection Officers by particularly significant classes of processors. Taken together, these are a significant selection of the innovative features of the GDPR.

Authors: Andin Aditya Rahman, Associate at Assegaf Hamzah & Partners, Indonesia, and Graham Greenleaf, PL&B Asia Pacific Editor.

This article expresses the personal views of A Rahman and does not necessarily reflect the opinion of his firm.

Emails: andin.rahman@ahp.co.id
graham@austlii.edu.au

2588 words

Electronic copy available at: https://ssrn.com/abstract=4343593