INDONESIA'S DP BILL LACKS A DPA, DESPITE GDPR SIMILARITIES

GRAHAM GREENLEAD AND ANDIN ADITYA RAHMAN

(20020) (164) Privacy Laws & Business International Report, 3-7
[2021] *UNSWLRS* 10

UNSW Law
UNSW Sydney NSW 2052 Australia

Indonesia's DP Bill lacks a DPA, despite GDPR similarities

Graham Greenleaf and Andin Aditya Rahman*

(2020) 164 *Privacy Laws & Business International Report* 1, 3-7

Indonesia's long-awaited comprehensive draft *Law on the Protection of Personal Data* ('the Bill') has been submitted by President Joko Widodo to the Chairperson of the Indonesian House of Representatives. Minister of Communication and Information, Johnny G. Plate announced the submission on 28 January 2020 and was summoned by the House to elaborate on the Bill in a formal meeting at the end of February, after which he stated that he expected the Bill will be the first legislation to be enacted by the House this year. Indonesian experts now expect delays as a result of the COVID-19 pandemic. An earlier version of a Bill had been released by the government in April 2019 ('2019 Bill'), with significant differences from this Bill.

Indonesia already has rudimentary data privacy laws, comprised primarily of an implementing Regulation 82 of 2012, which has since been repealed and replaced by Regulation 71 of 2019, made under the *Law on Information and Electronic Transactions* (Act No 11, 2008),[1] and since supplemented by Regulation 20 of 2016. These laws do not include a Data Protection Authority (DPA).

This article analyses the Bill in the context of other Asian data privacy laws and the EU's GDPR. It is based on an unofficial English translation, and informed by articles by Indonesian commentators.[2] All article references are to the Bill unless specified otherwise.

DPA missing in action

The most striking aspect of the Bill is that it fails to include what is generally considered to be the essential element[3] of a data privacy law: a separate, specialised (and usually independent) data protection authority (DPA). Only 10 of the 143 countries with data privacy laws omit a separate DPA. Some of them are in Asia, but only Taiwan purports to regulate public sector privacy without a separate DPA, and is examining creating one. Singapore and Malaysia have DPAs which are not independent of the Ministry in which they are based, but they are administratively separate from it, and (at least in the case of Singapore) have considerable expertise in data privacy issues, something not usually found in Ministries. A concentration of

* Graham Greenleaf is Professor of Law & Information Systems, UNSW Sydney and PLBIR Asia Pacific Editor. Andin Aditya Rahman is an Associate with the Indonesian law firm Assegaf Hamzah & Partners. andin.rahman@ahp.id. Valuable comments on this article have been received from Prof. Sinta Dewi of University of Padjadjaran, Bandung, Indonesia and Dr Clarisse Girot, Data Privacy Project Lead at Asian Business Law Institute (ABLI), Singapore d, but all responsibility for content remains with the authors.

[1] Graham Greenleaf and Sinta Dewi Rosadi 'Indonesia's data protection Regulation 2012: A brief code with data breach notification' (April, 2013) 122 *Privacy Laws & Business International Report*, pp. 24-27.

[2] Editors, Indonesian Law Digest 'The Draft Bill on Personal Data Protection - An Overview of Tighter Sanctions for Data Controllers and Data Processors' *Indonesian Law Digest* Issue 649, 12 February 2020, *Hukum Online Pro*.

[3] G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 73-74.

expertise and attention, as well as clear accountability for enforcement, are the main benefits of inclusion of a DPA.

All enforcement powers are in the hands of the Minister of Communication and Information, who will have the authority to regulate personal data processing (art. 17(3)), receive reports on data personal breaches (art. 40(1)), render administrative sanctions for non-compliance (art. 50(3)), and implement government measures for personal data protection (art. 58(2)).

Ministerial enforcement powers are a feature of Indonesia's current data privacy laws and regulations, and have been a conspicuous failure. There has been no Ministerial enforcement in seven years, except that several warnings have been issued[4]. This Bill may also be fated to be ignored, unless it has a DPA dedicated to its enforcement.

There have been quite a few earlier versions of a data privacy Bill drafted by the Indonesian government, but all have involved a specialised DPA. In a recent version, the Public Information Commission was going to act as the DPA, a combination of data privacy responsibilities with Freedom of Information/Right to Information (FOI/RTI) responsibilities, which is relatively common (for example, the UK ICO and Australia's OAIC). However, some influential Ministries objected, including on the grounds that Indonesia has too many separate agencies that do not function properly but are very costly to maintain.

Scope of the law

'Personal data' has a broad definition (art. 1(1)) as data which directly or indirectly identifies or makes identifiable (in combination with other information) an individual. Personal data is divided into that 'of a general nature' and that which is 'specific' (art. 3). 'Specific' data includes most categories commonly regarded as 'sensitive' (including biometric and genetic data), but not trade unionism, race or ethnicity, or religion or philosophical beliefs. 'Personal financial data' is however included, as is a capacity to extend the definition by regulations. The only consequence of data being defined as 'specific' is that it can result in the appointment of DPOs where processing is large-scale. Categorisation as being of a 'general nature' has no legal consequences. It is possible that regulations may make more distinctions between the two, such as placing more restrictive conditions on collection or use of 'specific' data, or higher security requirements.

'Processing' is defined broadly (art. 17(1)), and must be done in accordance with eight broad data protection principles (art. 17(2)), which may affect the interpretation of more detailed rights and obligations.

The Bill's obligations apply comprehensively, to individuals, corporations, public agencies and other institutions (art. 2). It has extra-territorial scope, not in the same way as the GDPR, but to processing occurring outside Indonesia which has legal consequences within Indonesia, and also applying to data owners who are outside Indonesia but are Indonesian citizens (art. 2). The scope of such extra-territoriality is unclear, as is its enforceability.

[4] One notable warning was to Facebook for unauthorized use of an estimated 1 million Indonesian nationals' personal data: Adam Prireza *Tempo.co* 'Govt Sends Second Warning Letters to Facebook' *Line Today* 12 April 2018 <https://today.line.me/id/pc/article/Govt%20Sends%20Second%20Warning%20Letters%20to%20Facebook-Govt+Sends+Second+Warning+Letters+to+Facebook-v5mYD5> . The Minister was satisfied with an audit conducted by Facebook after the second warning, and took no further action.

Grounds for lawful processing

Processing of personal data may only occur if it has a legitimate basis (similar to a fundamental aspect of the GDPR), which may be either based on consent (art, 18(1)) or on six non-consensual grounds (art. 18(2)).

Consensual processing must be based on a 'recorded written or oral agreement' (art. 19(1)) to 'one or more specific objectives' (purposes) communicated to the personal data owner (art. 18(1)).[5] Such consent must be 'clearly distinguished' (unbundled) from other consents, in an understandable and accessible format and in simple language (art. 19(4)) or it is not valid (art. 19(5)). Unlike the GDPR (art. 4(11)), there is no requirement that consent be 'freely given'. As in the GDPR (art. 5(1)(b)), multiple specific purposes are allowed. Eight complex items of notice[6] must be given to owners prior to their giving consent (art. 24(1)), and controllers must be able to show proof of consent (art. 24(2)). These 'notice and consent' requirement are quite strict, though less so than the GDPR.

The non-consensual bases for legitimate processing are (art. 18(2)):

a) to fulfil contractual obligations of the data controller or data owner;
b) to fulfil statutory obligations of the data controller;
c) to protect the vital interests of the data owner;
d) to implement the data controller's authorities provided by law;
e) to fulfil the data controller's obligations to provide public services (these last two are most relevant to public sector controllers);
f) to fulfil 'other legitimate interests', and to balance the interests of the data controller and the data owner.

Despite some ambiguities, these provisions aim to achieve objectives similar to the GDPR. However, only (f) requires balancing of the data owner's fundamental interests against the other interests involved, and there are no obligations to make such exceptions subject to requirements of proportionality (such as in GDPR art. 6(3)).

Rights of personal data owners

Indonesia has adopted the term 'personal data owner' (art. 1(5)), instead of 'data subject' (as found in many other countries' laws) as the possessor of statutory rights.[7] It is not clear that the concept of 'owner' means any more than that. Personal data owners have these rights:

(1) to ***access*** their personal data (art. 6), including to obtain details of who has accessed and used their personal data (art. 4);
(2) to ***update and correct*** their personal data (art. 7), including to complete it before it is processed (art. 5);
(3) to ***withdraw approval*** of processing (probably limited to data provided by the data owner) (art. 9);
(4) to ***postpone or limit processing*** 'in proportion to the purposes of processing' (art. 12);
(5) to ***halt processing***, delete and / or destroy their personal data (art. 8);

[5] The purpose specification principle is satisfied by this requirement, even though it is not explicit in the collection principle (art. 17(2)(a)).

[6] Legality; purpose; relevance; retention period; what is collected; period of processing; and owner's rights.

[7] One reason for this terminology is that 'data subject' does not translate comfortably into Bahasa.

(6) to object to the actions of decision-making based solely on ***automatic processing*** related to a person's profile (profiling) (art. 10);
(7) to choose ***pseudonymised processing*** for certain purposes (art. 11);
(8) to acquire from the data controller his/her personal data in a 'commonly used' format, and to use it (art. 14(1)); and to require the data controller to provide it in that format to another data controller (art. 14(2)); this is a strong '***data portability***' right.

These rights are stated very briefly, and may require clarification by regulations.

In order to exercise any of these first six rights, a data owner must first submit a written request to the data controller (art. 15), which is therefore the first step in any enforcement.

There are exceptions to the exercise of any of the last six rights in relation to these public sector interests: (a) defence and national security; (b) law enforcement processes; (c) the organization of the State; (d) financial systems supervisions; and (e) aggregate data processing for statistical purposes and scientific research within State administration. The vagueness of exception (c) raises dangers that the government will use it to obtain an unjustifiable degree of access to citizens' personal data, particularly as there will be no independent DPA to help restrain it from so doing.

Obligations of data controllers

Personal data controllers have numerous obligations, many of which reflect the above rights of data owners, but some of which are additional. One set of obligations concerns responsibility for the quality of personal data and of processing:

(1) to give the required ***notice*** when obtaining consent to processing, and be able to show proof of consent (art. 24);
(2) to ***process only in accordance with the purpose approved*** by the owner (art. 36); this reinforces the purpose specification principle in art. 18(1);
(3) to ***supervise processors*** under their control (art. 28);
(4) to ensure protection from unauthorized processing of personal data under its control (art. 29); the significance of this very general obligation is uncertain;
(5) to be responsible, and ***show responsibility***, for all data protection obligations (art. 41); this may be similar to 'demonstrable accountability' in the GDPR;
(6) to ***record all processing activities*** of personal data (art. 31);
(7) to ***appoint a data protection officer*** (DPO) where processing involves (a) public service activities; or (b) regular or systemic monitoring on a large scale; or (c) large scale processing of specific (sensitive) personal data; DPO qualifications are set out (art. 45); DPO duties are set out, and may be further specified in regulations (art. 46); What is 'a large scale' is not defined.
(8) to ***provide access*** to owners (including processing activities) within three days of request (art. 32); but to refuse access on specified grounds (adverse impacts on the owner, or on others, or on defence and national security) (art. 33);
(9) to ***update and/or correct*** personal data within 24 hours of request, and advise the owner (art. 34);
(10) to ***guarantee*** the accuracy, completeness and consistency of personal data, in accordance with regulations (art. 35); and in doing so, to 'conduct verification' (art. 35(2)), which may mean to do so with the data owner;

(11) to provide ***security*** to personal data, proportionate to the nature and risks of the data (art. 27); to prevent illegal accesses, by appropriate security measures, and in accordance with regulations (art. 30);
(12) to ***notify data breaches*** to both the owner and the Minister within 24 hours, and in some cases (to be specified) notify the public (art. 40).

Numerous obligations concern cessation of processing, or removal/destruction of data:

(13) to ***stop processing*** when consent is withdrawn, within three days (art. 25);
(14) to ***delay or suspend processing***, on request, for two days (art. 26);
(15) to ***discontinue processing*** when (a) the term of retention is reached, or (b) the processing objectives have been achieved, or (c) the owner requests, in accordance with regulations (art. 37);
(16) to ***remove (not destroy)*** personal data if (a) no longer required for purpose; or (b) owner withdraws consent; or (c) owner demands removal; or (d) obtained/processed illegally, in accordance with regulations (art. 38); but to restore the data if the owner requests (art. 38(3));
(17) to ***terminate (destroy)*** personal data if (a) no longer of value, or (b) both retention and archival periods expire, or (c) owner requests, or (d) not required for the completion of an on-going legal process (an illogical provision), in accordance with regulations (art. 39).

Obligations (15)-(17) appear to overlap, but in fact achieve different results: cessation of processing, removal of data (without destruction), and actual destruction. For example, regulations under arts. 37(1)(b), 38(1)(b) and 39(1)(a) will each in various ways implement the 'right to be forgotten' already included in the 2016 amendment to the Electronic Transactions law.[8] However, the differences between these obligations are not very clear.

Some of these controller obligations (arts. 32, 34, 37, 38(1)(a)-(c), 39(1)(c) and 40(1)(a)) do not apply where they conflict with interests of national defence and security, the law enforcement process, public interests in management of the State, and the financial system, but only insofar as regulations implement (art. 42).

Processor's obligations

The Bill imposes many of the above obligations directly on data processors, as well as on data controllers (those in arts. 21(1), 27-31, and 35) (art. 44). In addition, processors are obliged to only process personal data according to the instructions of the controller (or the articles applying directly to processors), and if they go beyond that, such processing will be the sole responsibility of the data processor (art. 43(4)), and the law will apply to them as it does to controllers.

Obligations on all persons

There are wide range of prohibitions on any person (including controllers and processors) doing certain things with personal data of others: collection to harm others, unlawful disclosure, unlawful use (art. 51); installing or operating processing of visual data in a public place or public service facility (art. 52); using visual data posted in public places or public service facilities to identify others (including face-recognition systems) (art. 53); falsifying personal data to obtain benefit, and selling or buying personal data (art. 54). These prohibitions are enforced as criminal offences (see below), and constitute the most serious breaches of the legislation.

[8] A. Rahman 'Indonesia enacts Personal Data Regulation' (February 2017) 145 *Privacy Laws & Business International Report* pp. 1, 6-9.

The Bill allows for the installation of visual data processors in public places or public service facilities, provided that it is for purposes limited to security, disaster prevention, or traffic organization/ analysis. Notice must be given in the area concerned, and it must not be used to identify persons (e.g. by face recognition), but with exceptions for crime prevention activities and law enforcement processes as prescribed by law (art. 22). The Bill defines 'public places' vaguely as 'facilities provided by the government, private entity, or person that are used for public activities'.

Data exports

The Bill allows exports of personal data from Indonesia in four situations (art. 49):

a) To countries (of the recipient's domicile) with a level of data protection to or higher than Indonesia's law. There is no mechanism for such countries to be identified, but regulations can be made (art. 49(2)) which would allow the government to specify a 'white list'.
b) Where there is an international agreement (presumably between States); this would include data protection Convention 108+, but presumably only if Indonesia was a party to it and therefore gained reciprocal obligations from other States (not possible without a DPA); APEC-CBPRs is not an agreement between States.
c) Where there are contracts between data controllers guaranteeing protection to the standard of the Indonesian law; regulations will need to specify some form of standard contractual clauses.
d) With the consent of the data owner. However, the notice given to data owners to obtain their consent to processing (art. 24(1)) does not include any details of proposed data transfers.

There are no data localisation provisions in this Bill. However, there are several Indonesian regulations already requiring data localisation.[9]

Enforcement

In the absence of a data protection authority (DPA), how is this Bill to be enforced? What remedies can data owners, or the public, obtain against data controllers and processors who have not complied with their obligations, or have breached the rights of data owners?

Complaints – For some rights, a request/complaint to a data controller must first be made (art. 15), but not for all rights, and not to enforce a controller/processor obligation. However, as yet, there is no explicit procedure in the Bill for individuals to make a complaint to the Minister about a breach, although this may be added later by regulations.

Administrative sanctions – Most of the obligations of controller and processors are capable of being enforced by administrative sanctions (art. 50(1)). The list of 25 articles found there does not include any of the rights of data owners, so their breach cannot directly result in administrative sanctions. The sanctions may be (a) written warnings; (b) suspension of

[9] See Justisiari P Kusumah and Danny Kobrata 'Jurisdictional Report – Indonesia' (paras. 47-57) in C. Girot (Ed.) *Regulation of Cross-Border Tansfers of Personal Data in Asia,* Asian Business Law Institute (ABLI) 2018 <https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia>. Since then, Government Regulation No.71 of 2019 (GR71) has replaced Government Regulation No. 82 of 2012 (GR82) in October 2019. 'ESPs for Public Purposes' may not process or store data outside Indonesia (with exceptions – Art20).

processing activities; (c) erasure or termination of data; (d) compensation; and/or (e) administrative fines (art. 50(2)). Sanctions are imposed by the Minister (art. 50(3)), with procedures to be detailed in regulations (art. 50(3)).

Administrative fines – Although art. 50(2)(e) enables the Minister to impose administrative fines, the Bill does not specify amounts, which must therefore await regulations being made. The extent to which the Bill has credibility depends on these regulations. The GDPR states that the criterion for fines are that they are 'dissuasive sanctions', but for dissuasion to be possible the maximum amounts of fines must be sufficiently high.

Compensation – The data owner 'has the right to demand and receive compensation for violation of his Personal Data in accordance with the provisions of the legislation' (art. 13). Broad and remedial interpretation of this provision would include both breaches of the obligations of data controllers or processors, and breaches of data owner rights. For the former, but perhaps not the latter, art. 50(2)(d) empowers the Minister to award compensation. It is unusual to see compensation as an administrative sanction in Indonesia; it is more often awarded by courts. At least some complainants, including those whose data owner rights have been breached, may need to seek compensation from a court instead. The Bill does not say whether they can so proceed because of a breach of art. 13, and it is possible that the right to seek compensation before a court may only apply where the government's own failures to comply are in issue. However, the Bill also provides that, where there is a prosecution of a corporation to enforce arts. 51-54 (discussed below), the court may add to the sentence 'payment for damages' (art. 66(4)(f)).

Rights of appeal and judicial review – The Bill does not explicitly provide any right of appeal against decisions of the Minister concerning administrative sanctions, but the State Administrative Court will have jurisdiction to examine such appeals, because such decisions are a form of a government-issued decree. In Indonesia, such reviews are like an appeal (rather than judicial review) because the Court can consider all aspects of the decision.

Criminal fines and imprisonment – There are no criminal fines or imprisonment applicable directly to breaches of their obligations by controllers or processors, but such breaches by them may also constitute the offences that any person can commit under arts. 51-54 discussed above. Articles 61-64 allow courts to impose penalties ranging from 10-70 billion rupiah (US$ 600,000 – US$ 4.2 million) for each of these offences. Appropriation of profits of crime is also possible (art. 66). Appeals against findings of criminal offences are available through the criminal justice system. Article 66 extends these offences to corporations and those who control them, with fines that can be tripled in the case of corporations, and a wide range of other enforcement measures available, including closing business activities temporarily or permanently. If these provisions were enforced strongly, they could be as significant as the separate obligations on controllers and processors.

As the Bill stands, it includes a wide range of enforcement measures in the forms of administrative sanctions by the Minister, and prosecutions before the Courts. However, data owners have much more limited rights to enforce the Bill, or to use the courts to ensure that it is enforced. Enforcement via courts may be a very lengthy process in Indonesia. Unless regulations create a system that data owners can use with confidence, it will all be left to the 'grace and favour' of the Minister, and therefore inspire little confidence that it will ever occur.

Conclusions: Trading influence for irrelevance

This Bill has many features which would, other than for the lack of a DPA, place it among the strongest data privacy laws of the fourteen Asian countries which have such laws. Its GDPR-

influenced rights of data owners, and obligations of data controllers and processors would make it one of the strongest data privacy laws in Asia, behind only South Korea and accompanying only Thailand and perhaps India (depending on its legislative process).

However, in the absence of a specialised (and credibly independent) Data Protection Authority, the law is likely to be inadequately (if at all) enforced, with the risk that it will be ignored by both data controllers and data owners. The international standing of Indonesia's law will be undermined a great deal by this omission: a positive adequacy finding by the European Commission is not likely;[10] accession to Convention 108+ will be impossible;[11] and the requirements for membership of organisations such as the Global Privacy Assembly (GPA) or Asia-Pacific Privacy Authorities (APPA) will not be met. Indonesia's law will have 'second class' status, and Indonesia will not have a 'seat at the table' in international discussions of data privacy policies. It will have traded influence for irrelevance.

[10] European Union General Data Protection Regulation (GDPR), art. 45(2)(b) requires the Commission to 'in particular, take account' of 'the existence and effective functioning of one or more independent supervisory authorities in the third countries'.

[11] Convention 108+ art. 15(5) requires supervisory authorities that 'act with complete independence'..