Indonesia introduces a comprehensive privacy Bill

The bill would be a benchmark for new laws and regulations in sectors not currently covered by sectoral laws. However no real progress is expected until 2017. **Andin Aditya Rahman** reports on the latest developments.

As a developing country, Indonesia has not yet implemented a comprehensive data privacy law, but has dispersed provisions on private data protection in various sectoral legal frameworks,[1] including the Data Protection Regulation 2012.[2]

The Indonesian government has now initiated the Draft Bill on the Protection of Private Data (Draft Bill),[3] which was prepared by the Ministry of Communication and Informatics for the 2016 Priority National Legislative Program.[4] The Draft Bill has yet to be discussed by the House of Representatives (House), and could be subject to further changes.

Despite this proposal by the Ministry of Communication and Informatics and the clear importance of the Draft Bill, based on currently circulating reports from the media, the Draft Bill will not be included into the 2016 Priority National Legislative Program,[5] and will likely be delayed until next year or the year after, considering the poor performance of the House last year, when it only managed to pass one substantive Bill.[6] The House could also adopt fewer laws than what is required by the 2016 Priority National Legislative Program, and have a significant number of Bills leftover that could delay the progress of the Draft Bill on the Protection of Private Data (Draft Bill), until 2017.

Regardless of this scepticism, should the Draft Bill be passed by the House, it will be the first umbrella legal instrument for Indonesia's privacy protection framework, and is likely to serve as the benchmark for new laws and regulations in other sectors that stipulate protection for private data. In addition, provisions in existing laws on disclosure of private data will remain valid only if they do not contradict provisions of the Draft Bill.

Overview

The Draft Bill includes provisions concerning classification and definition of private data, details on how private data are protected, obligations of private data administrators, private data transfers (domestic and overseas), a Data Protection Authority, and video surveillance devices. It also provides specific purposes that are, in principle, exempted from having to respect a person's right to privacy under certain conditions.

Classification and definition

Despite the importance of a clear-cut definition of what constitutes private data, currently prevailing laws and regulations fail to stipulate this matter in detail. The current version of the Draft Bill does not only provide a more extensive definition, but also adds a new classification of private data: sensitive private data.

Definition

The new definition of private data under the Draft Bill is more expansive compared to the existing definition under the Citizen Administration Law. Below is a comparison between the definitions.

Draft Bill

"Every data regarding the life of a person, whether identified and/or can be identified separately or in combination with other information, either directly or indirectly, through electronic and/or non-electronic systems."[7]

Citizen Administration Law

"Certain personal data of which the accuracy is kept, treated, and maintained, and of which the confidentiality is protected."[8]

Arguably, this disparity in defining private data could be as a result of having a different ultimate purpose. The Draft Bill is designed to be the umbrella law for the protection of privacy which requires a broader definition, whereas the Citizen Administration Law is mainly intended for the relevant government bodies to administer the data of Indonesian citizens, requiring protection from possible abuse by the government.

The Official Interpretation to the Draft Bill (regarded as part of the law in Indonesia) further provides that private data is "a living person's data, including but not limited to full name, passport number, photo or video, telephone number, electronic mail address, fingerprint sample, DNA profile and so forth, which can be used in combination to enable the identification of a person specifically that can lead to illicit disclosure which may weaken his/her right to privacy."

This further elaboration of the definition of private data will guarantee a person's right to keep confidential his/her full name, as well as personal documents and details as mentioned above, unless such is required by law or is requested as part of a law enforcement process.

Non-sensitive and sensitive personal data

As mentioned above, certain private [personal] data is further classified as sensitive private data, which is defined as "private data that requires special protection, which covers data related to a person's religion/beliefs, health, physical and mental condition, sexual matters, personal finance, and other private data that could potentially harm and cause detriment to the privacy of the data's subject."[9]

Sensitive private data can only be collected, processed, and disclosed based on written consent from the person that it relates to, and specifically for the following purposes:[10]

1. Protection of the person in question
2. Employment, medical, and law-enforcement purposes

3. Requested by authorized parties for the purpose of performing its functions based on prevailing laws and regulations; or
4. Is in the public domain due to actions undertaken by the person in question.

Other than these provisions, the Draft Bill does not add any further details regarding sensitive private data. There is no further elaboration of which 'other private data' could potentially harm and cause detriment to the privacy of a person (according to the definition). Furthermore, the Draft Bill does not elaborate the so-called 'special protection' in the definition of sensitive private data, or the procedures to claim such protection.

Protection of private data

Private data protection under the Draft Bill covers the phases of private data management quite comprehensively, from its collection to deletion.

'Private data administrators' are individuals, legal entities, business entities, government institutions, public agencies, or community organizations that carry out activities relating to private data, whether manually or using automatic data processing tools, in a structured manner and use a data storage system, which includes but not limited to obtaining, collecting, processing, analysing, storing, displaying, announcing, delivering, distributing and deleting private data.[11]

Collection

Of critical importance to the protection of private data, the Draft Bill stipulates procedures that must be complied with by private data administrators in collecting and managing private data.

Prior to the collection of any private data, the private data administrator must obtain the consent of the owner of the private data and disclose the following information:[12]

1. Legality of the private data administrator (proof that it is duly established with proper government documentation)
2. Purpose of collecting his/her private data
3. Types of private data that will be administered
4. Retention period of documents that will contain the private data
5. Details of what information is being collected
6. Period of time for which the private data will be administered and procedures in deleting the private data; and
7. Right of the owner of the private data to refuse to provide consent.

This requirement to secure consent of the private data subject is exempted if mandated as such by law, required to draft a contract with the private data subject, or necessary to ensure the safety or economic interests of the private data subject.[13]

The private data subject can withdraw his/her consent at any time, and the private data administrator cannot prevent or prohibit the private data subject from doing so, and must comply with such a request.[14]

Storage, access and correction

After collection, the data subject still retains various rights over his/her private data collected by the private data administrator. This includes the right to access the private data, and also modify, update or correct any inaccuracies, which must be fulfilled by private data administrators upon request.[15]

If the owner wishes to access his/her private data, the private data administrator must fulfil this request and also provide a log history relating to the administration of the private data in question over the past year. This request can be denied if it harms the safety or health of the private data subject or any other individual, will reveal another person's private data, or is against state interests.[16]

Deletion

Private data must be erased if the retention period has expired, it has served its purpose, or it is requested by the owner. The deletion of private data must also be in accordance with prevailing laws and regulations, and not be relevant to any case proceeding.[17]

Obligations of private data administrators

A private data administrator [data controller] must have a policy on the management of private data, and a standard operating procedure (SOP) covering steps that must be taken to protect the private data from damage or unlawful modification, disclosure, and processing, and the level of security needed to protect the private data. A private data administrator must also have an internal policy regarding the protection of private data information, which must be disclosed publicly.[18]

Moreover, the private data administrator must have an adequate security system to protect the private data from any unlawful access. It is important to duly comply with this provision considering that an owner of private data may claim for damages for any losses due to unlawful use of their private data.[19]

In case of any private data leak, the private data administrator must notify the data owner regarding:[20]

1. the private data which was revealed
2. the time and sequence of events that led to the private data leak
3. efforts by the private data administrator to address the private data leak; and
4. contact information of the private data administrator.

Data transfers

In addition to the above actions that require consent, the Draft Bill also obligates private data administrators to obtain consent from the owner in transferring his/her private data to another domestic party or overseas, unless an exemption is required based on a written notification from the Central Information Commission (Komisi Informasi Pusat).[21]

The Private Data Bill also requires the private data administrator to enter into an agreement with the private data recipient overseas. However, this is not required if:[22]

1. The Indonesian government has entered into an agreement regarding the exchange of private data with the government of the country where the private data is being transferred to; or
2. The country where the servers are located implements a similar or higher level of protection for private data as the Private Data Bill.

Transfers of private data may also occur during structural transactions of legal entities, such as mergers and acquisitions. In this case, private data subjects are required to be informed of any such structural transactions of the legal entity that possesses their private data.[23]

Data Protection Authority

The Public Information Commission (KIP) is to be the DPA, and will have authority to receive and act on complaints on all breaches of private data. As background information, the Public Information Commission was established in 2008 to ensure that the public has access to public information from government officials and may receive complaints when any person is denied their right to public information.

Video surveillance devices

A matter previously unregulated specifically in Indonesia's legal framework, but addressed by the Draft Bill is the use of video surveillance devices. The Draft Bill prohibits the use of such devices in public areas that might violate an individual's right to privacy, unless it is required based on prevailing laws and regulations or undertaken for the purpose of preventing or investigating criminal offences. The Draft Bill also exempts video surveillance devices installed for the purpose of preventing fires and accidents, as well as traffic management.[24] In areas where video surveillance devices are installed, the operator must prominently display an information sign that states whether there are video surveillance devices installed in the area.[25]

Exemptions

Although the right to privacy is an inherent human right, there are exceptions to this right under the Draft Bill, including national security and law enforcement. The right to privacy of a person is also exempted for news reporting, and scientific and statistical purposes, provided that the private data is obtained from published information. Specifically for news reporting, the private data must be obtained with the consent of the data owner.[26]

Even though these exceptions are well-intentioned, the conditions for news reporting, and scientific and statistical purposes, namely the source must be from published information, is oxymoronic. On the one hand, news reporting, and scientific and statistical purposes will take private data from the subjects and publish them as public information as news articles, research reports, journals, and so forth. If the Draft Bill then requires such private data to be acquired from published information, it can be questioned how the private data may be taken from the subjects so that it can be used as a source for news reporting, and scientific and statistical purposes.

Conclusion

The Draft Bill clearly provides a few new concepts concerning the protection of private data, including a different definition compared to that provided by the Citizen Administration Law, and a novel classification of private data (for Indonesia), namely sensitive private data. Unfortunately, the current version of the Draft Bill does not elaborate further regarding sensitive private data, and the supposedly special protection of sensitive private data or the procedures to claim such protection, rendering this classification of private data to be opaque.

Under the current version of the Draft Bill, critical fundamental rights are given to private data subjects, including the authority to request the deletion of their private data, and to modify, update or correct any inaccuracies. The main form of protection given by these rights is the consent requirement, which will at least provide control to the owner of the private data. This will prove to be essential for guaranteeing the right to privacy in Indonesia, a protection that has been severely lacking and left behind, despite being of critical importance in today's digital age where borders between public and private are gradually being blurred.

AUTHOR

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

REFERENCES

1 These include: Law No. 23 of 2006 regarding Citizen Administration, as amended by Law No. 24 of 2013 ("Citizen Administration Law"); Law No. 7 of 1992 regarding Banking, as amended by Law No. 10 of 1998; Law No. 36 of 1999 regarding Telecommunication.
2 Data Protection Regulation 2012 (Government Regulation No. 82 of 2012 regarding Organization of Electronic Systems and Transactions) made under Law No. 11 of 2008 regarding Electronic Information and Transactions; see Graham Greenleaf and Sinta Dewi 'Indonesia's Data Protection Regulation 2012: A Brief Code with Data Breach Notification' *Privacy Laws & Business International Report*, Issue 122, 24-27, April 2013.
3 Version (unofficial) in Bahasa Indonesian dated 15 October 2015 obtained for the purpose of this article: <http://www.hukumonline.com/pusatdata/detail/lt561f74edf3260/nprt/481/rancangan-uu-tahun-2015-perlindungan-data-pribadi>. English language version is not yet available.
4 Minister of Communication and Informatics of the Republic of Indonesia, "Kemkominfo Siapkan RUU Perlindungan Pribadi," 7 October 2015 (original article: GATRAnews, "Kemkominfo Siapkan RUU Perlindungan Data Pribadi," 6 October 2015).
5 Detikcom, "Paripurna DPR akan Sahkan Prolegnas 2016, Termasuk Revisi UU KPK," 26 January 2016.
6 The Bill on Guarantees, passed late December 2015, was the only legislation to be promulgated in 2015 that is considered to have material value compared to others that were only related to regional governance and ratification of international law instruments.
7 In Bahasa Indonesia: "Setiap data tentang kehidupan seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik." See: Article 1 (1) of the Draft Bill.
8 In Bahasa Indonesia: "Data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya." See: Article 1 (22) of the Citizen Administration Law.
9 In Bahasa Indonesia: "Data pribadi yang memerlukan perlindungan khusus yang terdiri dari data yang berkaitan dengan agama/keyakinan, kesehatan, kondisi fisik dan kondisi mental, kehidupan seksual, data keuangan pribadi, dan data pribadi lainnya yang mungkin dapat membahayakan dan merugikan privasi subjek data." See: Article 1 (3) of the Draft Bill.
10 Draft Bill, Art. 7 (2).
11 Draft Bill Art. 1 (9) juncto Art. 1 (6).
12 Draft Bill, Art. 15 (1) and (2).
13 Draft Bill, Art. 15 (4).
14 Draft Bill, Arts. 13, and 16 (1).
15 Draft Bill, Arts. 8, and Art. 9 jo. Art. 22.
16 Draft Bill, Art. 21 (1) and (3).
17 Draft Bill, Arts. 11 (2), and 27 (1).
18 Draft Bill, Arts. 19, 20, and 26.
19 Draft Bill, Arts. 25, and 12.
20 Draft Bill, Art. 29.
21 Draft Bill, Art. 35 jo. Art. 36 jo. Art. 1 (12).
22 Draft Bill, Art. 32.
23 Draft Bill, Art. 34.
24 Draft Bill, Art. 28 (1) and (2).
25 Draft Bill, Art. 28 (3).
26 Draft Bill, Art. 14.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK