ADVISORY
February 2020

MAKARIM & TAIRA S.
COUNSELLORS AT LAW

A GUIDE TO THE UPCOMING INDONESIAN DATA PROTECTION LAW (FINAL DRAFT LAW JANUARY 2020)

There had been several drafts of the law on Personal Data Protection until the final draft that was submitted by the Indonesian Government to the House of Representatives on 24 January 2020 ("**Final Draft Law**"). When passed, it will be Indonesia's first framework legislation to specifically deal with and serve as the 'umbrella regulation' on personal data protection.

This article discusses and summarizes the main provisions of the Final Draft Law, which hopefully will be passed as the new Personal Data Protection Law this year. The Final Draft Law has 72 Articles in 15 chapters covering the following topics:

1. the definition and types of personal data;
2. the rights of data subjects;
3. the processing of personal data;
4. the obligations of data controllers and processors when processing personal data;
5. transferring personal data;
6. administrative sanctions;
7. prohibitions against certain uses of personal data;
8. the establishment of behavior guidelines for personal data controllers;
9. the dispute resolution over the use of personal data;
10. international cooperation;
11. the roles of the government and the public; and
12. sanctions.

Given the broad scope of the Final Draft Law, this article only focuses on the key points of the Final Draft Law referred to in items 1 to 5 and 12 above and when relevant, discusses some differences between the Final Draft Law and the previous draft law circulated in April 2019 ("**April 2019 Draft**")

1. Defining Personal Data and Categories of Personal Data

The Final Draft Law defines personal data as *all data related to an identified and/or identifiable person which can be identified separately or combined with other information, directly or indirectly through electronic and non-electronic systems*. This definition mirrors the definition in the European General Data Protection Regulation ("**GDPR**")[1]. The academic script of the Final Draft Law reveals that some considerations, principles and rights are similar to those in the GDPR and the lawmakers sought inspiration from the GDPR for drafting this law.

[1] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation / "**GDPR**").

Makarim & Taira S.
Summitmas I, 16th & 17th Fls.
Jl. Jend. Sudirman Kav. 61-62
Jakarta 12190
Indonesia
P: (62-21) 5080 8300, 252 1272
F: (62-21) 252 2750, 252 2751
www.makarim.com

The Final Draft Law introduces the terms, "**Controller**"[2] and "**Processor**"[3] with the same meanings as in the GDPR. This is the first time an Indonesian regulation or law has used these terms as the previous Minister of Communications Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems does not use these terms. Under the Final Draft Law, only a natural person can be considered a Personal Data Subject.

The Final Draft Law introduces two types of personal data:

(i) General personal data

This data is the basic information about a Personal Data Subject, ie his/her name, gender, nationality, religion and combined personal data which identifies a person.

(ii) Specific personal data

This data includes a person's health data and information, biometric data, genetic data, sexual orientation, political view, criminal record, children's data, private financial data and/or other data specified under the prevailing laws and regulations. This specific or sensitive data may by its nature pose a risk to the Personal Data Subject when processed and therefore needs enhanced protection. The spirit of the GDPR regarding specific or sensitive data (the Final Draft Law takes the same approach) is that the processing of specific data is only lawful in a limited number of circumstances.

The April 2019 Draft did not consider different types of data as the Final Draft Law does now. The previous draft merely categorized general data as data that is publicly available when accessing public services, and specific personal data as the sensitive data of a person, the use of which requires the consent of the data subject. Clearly, the drafters of the law have now taken a similar approach to the GDPR and categorized data in the same way.

2. The Rights of Personal Data Subject

The Final Draft Law introduces several rights of Personal Data Subjects under Articles 4 to 14. Since most of these rights reflect the principles of and rights protected by the GDPR, we summarize the rights and similar provisions of the GDPR in comparison.

No	Type of Right	Articles of the Final Draft Law	Similar Articles in GDPR	Description
1.	The Right to be Informed	4	12, 13 and 14	The right to be informed the identity of party collecting the personal data, the legal basis for providing the information, and the purposes of the collection and processing of one's personal data.
2.	The Right to Complete Personal Data	5	5(1)d	The right to complete personal data being processed by a personal data processor. In GDPR, this right derives from the principle of data accuracy (personal data must be accurate and up-to-date) that a processor must apply when processing personal data.
3.	The Right to Access Data	6	15	The right to obtain data from a controller or to access data.

2 A **Controller** under the Final Draft Law is a party that determines the purposes and takes control of the processing of Personal Data.

3 A **Processor** under the Final Draft Law is a party that processes Personal Data on behalf of a Controller.

No	Type of Right	Articles of the Final Draft Law	Similar Articles in GDPR	Description
4.	The Right to Correct Data	7	16	The right to update and correct personal data if it is inaccurate.
5.	The Right to Erase Data	8	17	The right to halt personal data processing and delete or erase personal data. In the GDPR, this right is also known as the right to be forgotten[4], which is not absolute and only applies in certain circumstances.
6.	The Right to Object	9	21	The right to withdraw from personal data controllers the Personal Data Subject's consent to process personal data (eg for direct marketing purposes).
7	The Right to not have one's Data Processed Automatically	10	22	The right not to be subjected to automatic decision making, processing or profiling using one's personal data.
8.	The Right to Decide on the Processing of Personal Data Using a Pseudonym Mechanism	11	4(5), Recitals 26, 28 and 29	The right to decide on the processing of one's personal data using a pseudonym mechanism. Both the Final Draft Law and the GDPR define pseudonymization as a means of processing personal data in such a way that the personal data can no longer be attributed to a specific Personal Data Subject without the use of additional information, to ensure that the personal data is not attributed to an identified or identifiable natural person.
9	The Right to Delay or Limit Personal Data Processing	12	5(1)(e)	The right to delay or limit the processing of personal data according to the initial purpose for which the data is collected and processed. Under the GDPR, this right derives from the storage limitation principle which means that personal data must be processed as necessary and then deleted or made anonymous as soon as it is no longer needed for the purpose for which it was collected.
10.	The Right to File a Complaint and to Receive Compensation	13	77 and 82	The right to submit a complaint to the supervisory authority and to be compensated by the controller or processor for processing or storing personal data without the consent of the Data Subject.
11.	The Right to Data Portability	14	20	The right to obtain and transfer one's personal data from a controller in a common and legible digital format.
12.	The Right to Seek a Judicial Remedy	N/A	78 and 79	The right to an effective judicial remedy against a decision of a supervisory authority or Controller or Processor of one's personal data.
13.	The Right to Representation	N/A	80	The right to be represented by a non-profit agency when filing a complaint or receiving compensation.

4 'The right to be forgotten' in Indonesia can be found in Article 26(3) of Law No. 19 of 2016 on the Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (**EIT Law**) as well as in Articles 15 to 18 of Government Regulation No. 71 of 2019 on The Organization of Electronic Systems and Transactions, being the implementing regulation of the EIT Law.

If a Personal Data Subject wishes to enforce his/her rights under Articles 6 to 10 and 12 of the Final Draft Law, he/she must serve the personal data controller a written demand.

However, if the data is needed for the following purposes, the above rights (ie a Personal Data Subject's rights under Articles 8 to 12 and 14 of the Final Draft Law) cannot be exercised:

a. national defense and security;

b. law enforcement;

c. state administration;

d. data aggregation in which the personal data is processed for statistical and scientific purposes for state administration; or

e. the supervision of the financial or monetary sector, payment systems or financial systems stability.

The purpose in paragraph e above is new under the Final Draft Law. It was not included in the April 2019 Draft.

3. The Processing of Personal Data

According to the Final Draft Law, the processing of personal data includes the collection, analysis, storage, correction/ updating, displaying, publishing/announcing, transferring, transmitting, disclosing, deletion and removal of data. To process personal data, a valid consent of the Personal Data Subject is required, unless the personal data is to be processed for the following purposes:

i. for compliance with an agreement to which the Personal Data Subject is a party or the Personal Data Subject's request to comply with an agreement;

ii. the personal data controller's compliance with its obligations under the applicable laws and regulations;

iii. the protection of the Personal Data Subject's vital interests;

iv. the exercise of the personal data controller's authority in accordance with prevailing laws and regulations;

v. the personal data controller's compliance with its obligations related to public services; or

vi. the compliance with other lawful interests while considering the purposes, needs and interests of both the personal data controller and the Personal Data Subject's rights.

The Final Draft Law requires the consent of Personal Data Subject to be given explicitly (in writing or verbally with a voice recording). Consent can be given electronically or non-electronically. An agreement without an explicit consent clause can be considered null and void.

From the purposes in items i - vi above, it appears that prior to the drafting of the Final Draft Law, the existing regulations provide personal data protection mostly (if not always) by relying on the consent of the Personal Data Subject. The Final Draft Law finally introduces other purposes for personal data processing, including those for which valid consent is not required, presumably taken from the GDPR's provision on the legal grounds for personal data processing.

4. The Obligations of Personal Data Controllers and Processors When Processing Personal Data

Under the Final Draft Law, a personal data controller or processor can be a person, a public agency or organization/ institution.

When processing personal data, the personal data controllers have the following obligations:

i. to inform the Personal Data Subject of the purpose and legality of the data processing, his/her rights, details on the information collected, the types and relevance of the data processed and the processing and retention periods;

ii. to inform the Personal Data Subject of any change of information within 7 x 24 hours of the change;

iii. to halt the personal data processing within 3 x 24 hours of the receipt of the withdrawal of the consent by the Personal Data Subject;

iv. to delay or limit data processing within 2 x 24 hours of receipt of a delay/limit request from the Personal Data Subject;

v. to protect and ensure the security of Personal Data Subject's data, including from any unlawful processing of the personal data;

vi. to supervise all the parties involved in the data processing;

vii. to record all activities taking place during the data processing;

viii. to provide the Personal Data Subject access within 3 x 24 hours of receipt of his/her request for access;

ix. to update or correct personal data within 1 x 24 hours of receipt of a request to do so;

x. to halt the data processing upon the request of the Personal Data Subject, upon the expiry of the retention period, or when the purpose of the processing has been achieved;

xi. to delete personal data if the personal data is no longer necessary; the Personal Data Subject withdraws his/her consent; upon the request of the Personal Data Subject; or if the personal data was obtained and/or processed unlawfully;

xii. to remove personal data from its database if the data no longer serves any purpose; the personal data retention period has expired, upon the request of the Personal Data Subject; or if the personal data is not relevant to a legal proceeding;

xiii. in the event of a breach of the confidentiality of personal data, to inform the Personal Data Subject and Minister of Communication and Informatics within 3 x 24 hours of the occurrence of the breach;

xiv. to maintain the accuracy, completeness and consistency of personal data; and

xv. to process personal data in accordance with the processing purposes consented to by the Personal Data Subject.

The personal data controller's obligations in items viii to xiii (except for the deletion of personal data due to the unlawful processing of personal data and the removal of personal data due to the data no longer serves any purpose, the expiry of the personal data retention period or the data is not relevant to a legal proceeding) above do not apply if the data is needed in the interests of national defense and security, law enforcement, state administration, data aggregation for statistics/scientific purposes for state administration, and supervision of the financial or monetary sector, payment systems and financial systems stability.

The personal data processors have the following obligations:

i. to process personal data according to the personal data controller's orders or instructions;

ii. to maintain the confidentiality of the personal data while processing it;

iii. to ensure the security of personal data by using technical procedures and considering the nature and risk of the personal data;

iv. to supervise all the parties involved in the data processing;

v. to prevent personal data from being processed unlawfully;

vi. to prevent unlawful access to personal data;

vii. to record all the data processing activities; and

viii. to maintain the accuracy, completeness and consistency of personal data.

Personal data is processed under instructions and orders from a personal data controller, and therefore, liability during processing lies with the personal data controller. However, if a personal data processor processes personal data in a way contrary to or not covered by the personal data controller's instructions/orders, the personal data processor will be held liable for the personal data processing.

In the Final Draft Law, it is also introduced data protection officer, whose duties are to inform and give advice to the personal data controller or processor to comply with the provisions of the law, to monitor and ensure compliance with the law and the policies of the personal data controller or processor, to give advice on the impact of the personal data protection and to monitor the personal data controller and processor's performance and to coordinate and act as a contact person for issues related to the personal data processing. A data protection officer is required to be appointed if (i) the personal data processing is for public service purposes, (ii) the characteristics, scope and/or purposes of the main activities of the personal data controller require the regular and systematic supervision of personal data in large scale; and (iii) the main activities of the personal data controller consist of the personal data processing in large scale for specific personal data and/or personal data related to a crime.

5. Transferring Personal Data

Under the current regulations, the foreign country to which personal data is transferred is not required to meet certain criteria or have a certain level of personal data protection. However, under the Final Draft Law, a cross border data transfer is only allowed to a country or international organization that meets the following criteria:

a. it has an equal or higher level of protection compared to Indonesia;

b. it has entered into an agreement with Indonesia;

c. there is a binding contract between personal data controllers having standards and protection of personal data that are in line with the law; or

d. it has obtained the consent of the Personal Data Subject.

In the future, a separate government regulation will be issued to further regulate these criteria for a personal data transfer.

The above requirements for the transfer of personal data to a third party are somewhat similar to those under the GDPR, ie the existence of adequate data protection, contractual clauses, an international agreement or the Private Data Subject's consent. Without an implementing the regulation, the criteria for allowing a personal data transfer remain unclear. The issues that need further clarification (and will probably be covered by the upcoming government regulation) include for example, which authorized institution in Indonesia can issue the adequacy decision, the specifications of an international agreement and binding contracts which can satisfy the requirements for a transfer.

6. Administrative and Criminal Sanctions

The Final Draft Law imposes administrative and criminal sanctions for failing to provide sufficient personal data protection. The progressive administrative sanctions range from written warnings to a temporary suspension of activities, the deletion or removal of personal data, compensation and/or a fine.

The criminal sanction under the April 2019 Draft was a fine, while the Final Draft Law now imposes the additional sanction of imprisonment. Under the Final Draft Law, the fine ranges from Rp10,000,000,000 to Rp70,000,000,000 and the imprisonment ranges from one year to seven years.

In addition to a fine and imprisonment, the additional criminal sanctions of the confiscation of the perpetrator's benefits and/or wealth obtained and resulted from the crime and compensation may be imposed.

* * * * *

Contacts:

Brinanda Lidwina Kaliska - brinanda.kaliska@makarim.com
Kurniawan Tanzil - kurniawan.tanzil@makarim.com