ADVISORY
17 January 2017

MAKARIM & TAIRA S.
COUNSELLORS AT LAW

New Regulation on the Protection of Personal Data: Key Provisions

At the end of 2016, the Minister of Communication and Informatics issued Regulation No. 20 of 2016 on Personal Data Protection within Electronic Systems ("**Regulation 20/2016**") to implement Article 15 (3) of Government Regulation No. 82 of 2012 on the Organization of Electronic Systems and Transactions ("**GR 82/2012**"). The regulation was issued on 7 November 2016 and came into force on 1 December 2016. Existing electronic system providers must adjust to the regulation within 2 years of its issuance.

Regulation 20/2016 provides, among other things, a definition of personal data, which is not fully defined in GR82/2012. It is therefore a key regulation on what constitutes personal data in electronic system under Indonesian law and how it must be protected.

Personal Data

Personal data is defined as certain individual data that is stored, maintained, and its veracity is sustained, the confidentiality of which must be protected. Further, Regulation 20/2016 defines certain individual data as accurate and concrete information which is directly or indirectly attached to and identified with an individual, the use of which must conform to the prevailing laws and regulations.

From the above definition, all identifiable data about an individual provided to the electronic system provider without a clear scope, category or specifications should be considered personal data.

Personal Data Protection

Personal data must be protected through and during its receipt, collection, processing, analysis, storage, display, publication, transmission, dissemination and deletion. One of the key personal data protection principles under the regulation is that personal data must be considered an aspect of privacy and therefore be treated as confidential information. The use of personal data requires the owner's written consent, given either manually or electronically, and/or must be allowed under the applicable laws and regulations. The written consent may be given after the veracity, confidentiality and purpose for which the personal data will be processed have been confirmed by the owner. If the owner is not legally able to provide his/her consent, it must be obtained from his/her biological parents or authorized guardians.

Below are some main mandatory measures to be taken when dealing with personal data in a verified electronic system:

Actions	Mandatory Measures
Receipt and Collection	• The owner's written consent is mandatory; • The electronic system provider must provide a consent form in Indonesian for obtaining the consent of the owner of the personal data; • Unless expressly stated otherwise, personal data must always be treated as confidential;

Makarim & Taira S.
Summitmas I, 16th & 17th Fls.
Jl. Jend. Sudirman Kav. 61-62
Jakarta 12190
Indonesia
P: (62-21) 252 1272, 520 0001
F: (62-21) 252 2750, 252 2751
E: info@makarim.com
www.makarim.com

Actions	Mandatory Measures
	• The electronic system provider can only obtain relevant information in accordance with the purposes of its usage; • Data received must be verified with the owner or other reliable sources; • The electronic system must have a feature that allows the owner to declare that the personal data is or is not confidential and to amend, add to, or update it.
Processing and Analysis	• The purpose for which the personal data is to be processed and analyzed must be stated clearly before its collection; • The owner's written consent is required, except for personal data which has been publicly displayed or published; • These are limited to verified personal data.
Storage	• The electronic system provider should keep verified personal data in encrypted form; • The data should be stored for at least 5 years or as specified under the prevailing rules and regulations; • The data may be deleted upon expiry of the storage period, unless the data is still being used for the intended purposes; • The data center and disaster recovery center must be located in Indonesia.
Display, Announcement, Transmission, Dissemination and/or Opening of Access	• The owner's written consent is required; • It must only be for the stated intended purposes; • Relevant and required personal data must be provided to law enforcement agencies in accordance with the prevailing rules and regulations; • The use and utilization of personal data displayed, announced, transmitted, and disseminated by the electronic system provider must be based on the owner's written consent. Such use and utilization must conform to the purpose of the receipt, collection, processing, or analysis of the personal data.
Deletion	• Personal data may only be deleted: - upon the expiry of the storage period under Regulation 20/2016 or according to the storage period specified in the relevant regulation; or - at the request of the data owner; • The deletion must be done against the documents related to the personal data (partly or wholly) in both the electronic and the non-electronic forms of the personal data based on consent from the data owner or in accordance with the laws and regulations so that the personal data cannot be displayed in the electronic system again, unless the owner provides new personal data.

Cross-Border Transmission of Personal Data

Regulation 20/2016 requires the trans-border transmission of personal data to be coordinated with the authorized Minister or officials and comply with the prevailing rules and regulations on the trans-border transmission of personal data. The trans-border transmission of personal data is to be coordinated through:

- providing a plan for the transmission of personal data containing at least the clear name of the receiving country, the recipient, the transmission date and the purpose for which the personal data is being transmitted;
- requesting an advice from the authorized Minister or official, if necessary; and
- submitting a report on the trans-border transmission of the personal data to the Minister.

To date, no regulation on the trans-border transmission of personal data has been issued. Therefore, in the absence of the regulation, the trans-border transmission must be further discussed with the relevant Minister or official.

Obligations of Electronic System Providers

Regulation 20/2016 imposes several obligations on electronic system providers, among other things:

- electronic system providers must have their electronic system certified following the procedure under the prevailing laws and regulations.
- electronic system providers must have internal procedures for protecting personal data.
- electronic system providers must deliver a written notification within 14 days of any failure in the system to protect the confidentiality of personal data.

Dispute Settlement

As an alternative for dispute settlement mechanism, Regulation 20/2016 provides an amicable dispute settlement through the Minister. A personal data owner with a complaint can submit a report to the Minister within 30 days of finding out that:

1. the electronic system provider has failed to deliver him/her a written notification of a failure to maintain the confidentiality of his/her personal data, whether the failure has the potential to cause him/her to suffer a loss or not; or
2. the owner has suffered a loss because of the failure to maintain the confidentiality of his/her personal data and received the notification of the failure too late.

The Minister should have the dispute resolved amicably within 14 days of receipt of the complete report and information. If this fails, the owner has the right to file a civil lawsuit.

Administrative Sanctions

The following administrative sanctions may be imposed on any person for the unauthorized receipt, collection, processing, analysis, storage, display, publication, transmission and/or dissemination of personal data:

1. oral warnings; followed by
2. written warnings;
3. a suspension of all activities; and/or
4. an online notice of its unauthorized activities.

* * *

Makarim & Taira S.
17 January 2017