DATA PROTECTION
LAWS OF THE WORLD
Indonesia

DLA PIPER

Downloaded: 16 January 2020
IN INDONESIA:

DATA PROTECTION LAWS OF THE WORLD

LAW

Specific Regulations

In Indonesia, as of the date of this publication there is no general law on data protection. However, there are certain regulations concerning the use of electronic data. The primary sources of the management of electronic information and transactions are Law No. 11 of 2008 regarding Electronic Information and Transactions (EIT Law) as amended by Law No. 19 of 2016 regarding the Amendment of EIT Law (EIT Law Amendment), Government Regulation No. 82 of 2012 regarding Provisions of Electronic systems and Transactions (Reg. 82) and its implementing regulation, Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI Regulation).

However, a new draft Bill on the Protection of Private Personal Data (the Bill) is being discussed and as of this date it has not been issued. Although the exact date remains uncertain and the Bill is still to be considered by the House of Representatives, if passed, this will become Indonesia’s first comprehensive law to specifically deal with the issue of data privacy.

In addition to the provisions under EIT Law, Reg. 82 and MOCI Regulation, there are also a series of regulations which also cover certain provisions which may relate to data protection, such as:

Telecommunications Sector

Article 40 of Law No. 36 of 1999 regarding Telecommunications (‘Telecommunications Law’) provides that any person is prohibited from any kind of tapping of information transmitted through any kind of telecommunications network. Article 42 of the Telecommunications Law stipulates that any telecommunications services operator has to keep confidential any information transmitted or received by a telecommunications service subscriber through telecommunications networks or telecommunications services provided by the relevant operator.

Public Information Sector

Article 6 of Law No. 14 of 2008 regarding Disclosure of Public Information provides that information relating to personal rights may not be disclosed by public bodies. Article 17 of the relevant law, together with other laws, prohibits the disclosure of private information of any person, particularly that which concerns family history; medical and psychological history; financial information (including assets, earnings and bank records) and evaluation records concerning a person’s capability, recommendation, intellectual, formal, or informal education records.

Banking and Capital Markets Sectors

Data privacy in this sector is regulated under Law 7 of 1992 as amended by Law 10 of 1998 on Banking (‘Banking Law’) and Law 8 of 1995 on Capital Markets (Capital Markets Law) respectively. The regulations apply to both individuals and corporate data.
Bank Indonesia’s Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilization of Information Technology by the Bank stipulates that the bank’s customer data transfer (by way of establishing a data center or data processing outside the Indonesia territory) necessitates prior approval being obtained from Bank Indonesia.

**DEFINITIONS**

**Definition of personal data**

Reg. 82 and MOCI Regulation defines Personal Data as: data of an individual, which is stored, maintained and which correctness is preserved and of which its confidentiality is protected (including under the EIT Law and Reg 82).

**Definition of sensitive personal data**

Currently, there is no specific definition on sensitive personal data under the prevailing laws and regulations.

**NATIONAL DATA PROTECTION AUTHORITY**

There is no national data protection authority for data privacy in general in Indonesia.

For example, the Indonesian Financial Services Authority ('FSA') has the authority to act as the regulator of data privacy in the capital markets sector (since December 31, 2012) and with regard to banks' customer data privacy issues (since December 31, 2013).

However, please note that article 65 of Reg. 82 provides that a business enactor who operates electronic transactions may be certified by a Competence Certification Body (Lembaga Sertifikasi Keandalan) which may be a domestic Indonesian (but currently no such domestic bodies exist) or foreign competence certification body.

**REGISTRATION**

Minister of Communication and Informatics Regulation No. 36 of 2014 regarding Procedures of Electronic System Provider Registration (MOCI Reg 36) differentiates electronic system providers into electronic system provider for public services and electronic system provider for non-public services. An electronic system provider for public services must conduct registration, while an electronic system provider for non-public services may conduct registration, which suggests registration is not mandatory for an electronic system provider for non-public services).

MOCI Reg 36 specifically states that electronic system providers for public services are legal entities related with the government for example state institutions, government agencies, corporations in the form of state-owned enterprises, regional government-owned enterprise, or other legal entities in relation with state’s mission.

Electronic system providers for non-public services are not specifically defined under MOCI Reg 36, but in general other legal entities that are not related with government, such as private corporations, can be classified as electronic system providers for non-public services.

However, the regulators interpret ‘public service’ in regards to electronic system provider pursuant to Government Regulation No. 96 of 2012 regarding Implementation of Law No. 25 of 2009 regarding Public Service (GR No. 96).

GR No. 96 defines Public Service as an activity or chain of activities in terms of fulfilling the service needs in accordance with the law and regulation for every citizen and individual on goods, services, and / or administrative services that are provided by the public service operator. GR No. 96 further defines Public Service Operator as every state operator institution, corporation, independent institution that are formed based on laws for public service activity, and other legal entities that are formed only for the public service activity. Law No. 25 of 2009 regarding Public Services (Law No. 25). Article 5 (1) of Law No. 25 provides that the scope of public services includes public goods and services as well as administrative services. Article 5(2) of Law No. 25 further provides that this includes education, teaching, work and business, housing, communication and information, environment, health, social security, energy, banking, transportation, natural resources, tourism and other strategic sectors.

In relation to the above, an electronic system provider for non-public services falls under the corporation (non-government
related legal entity), providing service for every citizen / individual. Therefore, an electronic system provider for non-public services is also considered as public services pursuant to GR No. 96.

Consequently, all electronic system providers, whether for public services or non-public services, must conduct registration.

Article 4 of Minister of Communications and Informatics Regulation No. 4 of 2016 regarding Management System of Information Protection (MOCI Reg. No. 4/2016) provides that there are three categories of electronic systems: (i) strategic electronic system, which is an electronic system that causes serious impact to the public interest, public services, state governance stability, or state defense and security; (ii) high electronic system, which is an electronic system that causes limited impact to the interest of certain sector and / or territory; and (iii) low electronic system, which is any other electronic system aside from strategic and high electronic systems.

Article 10 of MOCI Reg. No. 4/2016 provides that strategic and high electronic system providers (for public services) must obtain a Certificate of Management System of Information Protection, while low electronic system providers (for public services) may obtain Certificate of Management System of Information Protection.

DATA PROTECTION OFFICERS

There is no requirement in Indonesia for organizations to appoint a data protection officer.

COLLECTION & PROCESSING

EIT Law, Reg. 82 and the MOCI Regulation specifically regulates the obligation to obtain "consent" from the owner of the personal data in the case of data collection, use and processing. Article 7(1) of MOCI Regulation regulates that in obtaining and collecting Personal Data the electronic system provider must also be limited to the relevant and suitable information in accordance to its purpose and must be conducted accurately. Article 12(1) of MOCI Regulation also regulates that Personal Data can only be processed and analyzed in accordance with the needs of the electronic system provider that have been stated clearly at the time the Personal Data is obtained and collected.

Reg. 82 provide the specific provisions on the obligation for Electronic System Providers to public services to set up a data center and disaster recovery center in Indonesia, namely:

- Before an Electronic System for public services is implemented, the provider of an Electronic System must register with the Minister of Communication and Information and Technology (MOCI).
- In the provision of an Electronic System, the provider should ensure secrecy, totality and the availability of the Personal Data it manages. The provider should also ensure that the collection, the consumption and usage of Personal Data is based on the consent of the Personal Data owner, except if regulated otherwise. (Article 15(1)(b) of Reg. 82). The provider should ensure that the usage or disclosure of data is done based on consent and is in line with the objectives as disclosed to the relevant owner at the time of obtaining the data. (Article 15(1)(c) of Reg. 82).
- The provider of the Electronic System is also obliged to provide audit track records of the Electronic System.

TRANSFER

Article 22(2) of Reg. 82 regulates the transfer of data, which provides in any case that in the implementation of an Electronic System or Electronic Document aimed to transfer Electronic Information or Electronic Document, the Electronic Information or Electronic Document must be unique and (the provider shall) explain the control and possession of the Electronic Information or Electronic Document.

Article 21(1) of MOCI Regulation states that displaying, announcing, transferring, broadcasting, or opening Personal Data access in the Electronic System can only be conducted:

- By Consent (being defined as a written agreement either manually or electronically being given by the owner of Personal Data after obtaining a full explanation regarding the process for acquiring, collecting, processing, analyzing, storing, displaying, announcing, disseminating and sending, including the confidentiality or non-confidentiality of the Personal Data), except as otherwise stipulated by laws and regulations, and
After its accuracy and compatibility with the purpose of obtaining and collecting such Personal Data is verified

Article 22(1) of the MOCI Regulation states that transferring Personal Data that is managed by an electronic system operator at the government and regional government institution including the public or private sector domiciled in the territory of Indonesia to [parties] outside the territory of Indonesia must:

- Coordinate with the MOCI or the official or institution being authorized for such purpose, and
- Implement the laws and regulations regarding the transboundary exchange of Personal Data

The implementation of the coordination as stipulated in Article 22(1)(a) of MOCI Regulation are:

- To report the implementation plan of Personal Data transfer, at least containing the clear name, designated country, recipient subject name, implementation date, and reason / purpose of the transfer
- To request for advocacy, if needed
- To report the activities implementation result

SECURITY

The obligations of Electronic System Providers are regulated under Reg. 82 and MOCI Regulation, which include:

- Guarantee the confidentiality of the source code of the software
- Ensure agreements on minimum service level and information security towards the information technology services being used as well as security and facility of internal communication security it implements
- Protect and ensure the privacy and personal data protection of users
- Ensure the appropriate lawful use and disclosure of the personal data
- Provide data center and disaster recovery center (for Electronic System Providers for public services)
- Provide the audit records on all Provision of Electronic Systems activities
- Provide information in the Electronic System based on legitimate request from investigators for certain crimes
- Provide options to the Personal Data Owner regarding the Personal Data that is processed so that [the Personal Data] can or cannot be used or displayed by a third party based on the Consent as long as it is related with the purpose of obtaining and collecting the Personal Data
- Provide access or opportunity to the Personal Data Owner to change or renew their Personal Data without disturbing the system management of the Personal Data, except as otherwise regulated by laws and regulations
- Delete the Personal Data if: (i) it has reached the maximum period of storing the Personal Data (at the shortest five years or based on the applicable regulations / specific sectoral regulations); or (ii) by request from the Personal Data Owner, except as otherwise regulated by laws and regulations, and
- Provide a contact person that is easy to be contacted by the Personal Data Owner in relation to their Personal Data

In the telecommunication sector, Article 19 of Minister of Communication and Informatics Regulation No. 26/PER/M.KOMINFO/05/2007 regarding the Security and Utilization of Internet Protocol based Telecommunications Network (as amended) (MR 26/2007) also provides that the telecommunication service provider is responsible for data storage due to its obligation to record its log file for at least three months.

BREACH NOTIFICATION

Article 15(2) of Reg. 82 provides that the provider of an Electronic System must provide written notification to the owner of personal data upon its failure to protect the personal data.

Article 20(3) of Reg. 82 states that the provider of an Electronic System must make the utmost effort to protect personal data and to immediately report any failure or serious system interference or disturbance to a law enforcement official or the Supervising and Regulatory Authority of the relevant sector.

Article 28(c) of the MOCI Regulation provides that a written notice to the Personal Data Owner is required if there is a failure in protecting the secrecy of the Personal Data in the Electronic System. The provisions of the notice are as follows:
• Must provide the reason or cause of the occurrence of the failure in protecting the secrecy of Personal Data. This can be provided electronically, if the Personal Data Owner has given Consent for it at the time of obtaining and collecting their Personal Data
• Must ensure that the notice has been received by the Personal Data Owner if the failure contains potential loss to the relevant Personal Data Owner, and
• The written notice is sent to the Personal Data Owner no later than 14 days after the failure is discovered

ENFORCEMENT

In Indonesia, the sanctions for breaches of data privacy are found under the relevant legislation and are essentially fines. Imprisonment may be imposed in severe instances, such as in the event of intentional infringement.

The EIT Law and EIT Law Amendment provides criminal penalties ranging from:

• Rp600 million fine to Rp800 million and six to eight years imprisonment for unlawful access
• Rp800 million fine and 10 years imprisonment for interception or wiretapping of a transmission
• Rp2 billion to Rp5 billion and 8 to 10 years imprisonment for alteration, addition, reduction, transmission, tampering, deletion, moving or hiding Electronic Information or Electronic Records

Failure to comply with Reg. 82 is subject to administrative sanctions (which do not eliminate any civil and criminal liability). These administration sanctions are in the forms of:

• Written warning
• Administrative fines
• Temporary dismissal
• Expulsion from the list of registrations (as required under the regulation)

Failure to comply with MOCI Regulations is subject to administrative sanctions in the form of:

• Verbal warning
• Written warning
• Temporary dismissal of activities
• An announcement in the online website

Banking Law

Under Article 47 of the Banking Law, any commissioner, director or employee of a bank or its affiliates who intentionally provides information which has to be kept secret may be sentenced to imprisonment for not less than 2 years but not more than 4 years, and fined at least Rp4 billion but not more than Rp8 billion.

Capital Markets Law

Under Capital Markets Law, the Financial Services Authority (Previously BAPEPAM LK) is empowered to impose the following administrative sanctions for breaches of the provisions dealing with data protection. The sanctions include:

• A written reminder
• A fine
• Limitations on business
• Suspension of business
• Revocation of business license
• Cancellation of approval
• Cancellation of registration

ELECTRONIC MARKETING

EIT Law and Reg. 82 do not specifically address electronic marketing. Article 25 of the EIT Law provides that an Internet website,
among other things, is acknowledged and protected as an Intellectual Property (IP) and consequently, should fall under the ambit of the relevant IP laws, which may in certain cases fall under the Indonesian Copyright Law.

**ONLINE PRIVACY**

There are currently no laws and regulations concerning cookies and location data. However, if the data collected by cookies or location data is obtained by the unlawful access of another party’s electronic information, this is subject to six to eight years imprisonment and / or a fine of Rp600 million to Rp800 million.

**KEY CONTACTS**

Ivan Almaida Baely & Firmansyah  
www.iab-net.com

- **Erwin Purba**  
  Partner  
  T +62 21 5790 5090  
  erwin.purba@iab-net.com

- **Robert Hasan**  
  Associate  
  T +62 21 5790 5090  
  robert.hasan@iab-net.com

- **Fariz Ghassen**  
  Associate  
  T +62 21 5790 5090  
  fariz.ghassen@iab-net.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.