INDONESIA

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. 71 of 2019 regarding Provisions of Electronic Systems and Transactions (“Reg. 71”) and its implementing regulation, Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (the “MOCI Regulation”).

However, for a number of years, a new draft Bill on the Protection of Private Personal Data (the “Bill”) is being discussed but to 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. 71 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. Furthermore, 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 / 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.
Finanical Services Authority Regulation No. 38/POJK.03/2016 on the Implementation of Risk Management in the Utilisation of Information Technology by the Bank stipulates that the bank’s customer data transfer (by way of establishing a data centre or a data processing outside Indonesia territory) necessitates prior approval being obtained from the Financial Services Authority (OJK).

DEFINITIONS

Definition of personal data

Reg. 71 defines Personal Data as any data of an individual who can be identified from that data, or from that data when combined with other information both directly or indirectly through electronic or non-electronic systems.

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 31 December 2012) and with regard to banks’ customer data privacy issues (since 31 December 2013).

However, please note that article 73 of Reg. 71 provides that a business enactor who operates electronic transactions may be certified by a Competence Certification Body (Lembaga Serifikasi Keandalan) which may be a domestic Indonesian (but currently no such domestic bodies exist) or foreign competence certification body.

REGISTRATION

Pursuant to Article 2 (2) of Reg. 71 an “Electronic System Provider” is either a:

1. Public Scope Electronic System Provider; or
2. Private Scope Electronic System Provider.

“Public Scope Electronic System Provider” includes:

- the Agency[1]; and
- an Institution appointed by the Agency.

The term Public Scope Electronic System Provider does not include any regulatory or supervisory authority in the finance sector.

According to Article 2 (5) Reg. 71, the term “Private Scope Electronic System Provider” includes:

- an Electronic System Provider that is regulated or supervised by a Ministry or Agency based on statutory provisions; and
- an Electronic System Provider that has a portal, site, or application in the network through the internet that is used to:
  - provide, manage, and / or operate, offer and / or trade goods and / or services;
  - provide, manage, and / or operate finance transaction services;
  - deliver material or paid digital content through data networks both by way of downloading through a portal or site, delivery via electronic mail, or through other application to the user’s device;
  - provide, manage, and / or operate communication services including but not limited to short messages, voice calls, video calls, electronic mails, and conversations within the network in the form of digital platforms, networking services and social media;
  - search engine services, Electronic Information provisioning services in the form of text, sound, picture, animation, music, video, movie, and game or combination of several and / or all of them; and / or
  - processing of Personal Data for community service operational activities related to the Electronic Transaction
Article 6 Reg. 71 regulates that both Public Scope Electronic System Providers and Private Scope Electronic System Providers are obliged to conduct registration. The registration shall be submitted through electronically integrated business licensing services in accordance with the statutory provisions and it must be done before the Electronic System is used by the Electronic System User.

Furthermore, 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 such as: (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.

Footnote 1: Being defined as a legislative, executive and judicative agencies at the central and regional level and other agencies that are formed by the laws.

DATA PROTECTION OFFICERS

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

COLLECTION & PROCESSING

Based on Article 14 (2) of GR. 71, processing of personal data includes:

- obtainment and collection;
- processing and analyzing;
- storing;
- correction and updates;
- displaying, announcing, transferring, distributing or disclosure; and / or
- deletion or removal.

As the general rule to process personal data, EIT Law, Reg. 71 and the MOCI Regulation specifically regulates the obligation to obtain “consent” (as defined below) from the owner of the personal data. Furthermore, 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 analysed 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.

An Electronic System Provider shall also implement the principles of Personal Data protection in the processing of Personal Data which includes [1]:

- Personal Data collection is conducted in a limited and specific manner, legally valid, fairly, with the knowledge and approval of the Personal Data owner;
- Personal Data processing is conducted in accordance with its purpose;
- Personal Data processing is conducted by securing the rights of the Personal Data owner;
- Personal Data processing is conducted accurately, completely, not misleading, up to date, can be accounted for, and by taking into account to the purpose of processing of the Personal Data;
- Personal Data processing is conducted by protecting the security of Personal Data from loss, misuse, unauthorized access and disclosure, as well as the alteration or destruction of Personal Data;
• Personal Data processing is conducted by notifying the purpose of collection, processing activities, and failure of Personal Data protection; and
• Personal Data processing is destroyed and/or deleted except if it is still in the retention period in accordance with the necessity based on the laws and regulations.

Footnote 1: Article 14 (1) of Reg. 71.

TRANSFER

Article 26 (2) of Reg. 71 provides that in the implementation of the Electronic System which aims to Electronic Information and/or Electronic Document that can be transferred (such as securities in electronic form), such Electronic Information and/or Electronic Document must be unique and explain the possession and ownership.

The elucidation of Article 26 (2) of Reg. 71 further explains the above provision, as follows:

- “Electronic Information and/or Electronic Document must be unique” means it is the only one that represents a certain value.
- “Electronic Information and/or Electronic Document must explain the possession” means the Electronic System has control system or recording system over such Electronic Information and/or Electronic Document.
- “Electronic Information and/or Electronic Document must explain the ownership” means the Electronic System has technology control measure that guarantees such Electronic Information and/or Electronic Document only has single authoritative copy and cannot be amended.

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

- By Consent (being defined as a written agreement either manually and/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, storing, dis-playing, announcing, sending, and disseminating including the confidentiality or non-confidentiality of the Personal Data), except stipulated otherwise 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 provider 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; and
- To report the activities implementation result.

SECURITY

The obligations of Electronic System Providers are regulated under Reg. 71 and MOCI Regulation, which amongst other things shall:

- 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 implement;

- protect and ensure the privacy and personal data protection of users;
- ensure the appropriate lawful use and disclosure of the personal data;
- provide the audit records on all Provision of Electronic Systems activities;
- have governance policies, operational work procedures, and audit mechanisms that are conducted periodically in the Electronic System;
- for Private Scope Electronic System Providers who process and/or store Personal Data outside of Indonesia, must ensure the supervisory effectiveness of the Ministry or Agency and law enforcement.
- provide access to the electronic system for the purpose of supervision and law enforcement.
- 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 and / or displayed by / at 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 Personal Data Owner to change or renew his/her Personal Data without disturbing the system management of the Personal Data, except regulated otherwise by laws and regulations;
- delete the Personal Data if (i) it has reached the maximum period of storing the Personal Data (at the shortest 5 years or based on the applicable regulations/ specific sectoral regulations); or (ii) by request from the Personal Data Owner, except regulated otherwise by the laws and regulations; and
- provide contact person that is easy to be contacted by the Personal Data Owner in relation to his / her 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 Utilisation 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 14 (5) of Reg. 71 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 24 (3) of Reg. 71 provides that the provider of an Electronic System must make the utmost effort to protect personal data and to immediately report any failure / serious system interference / disturbance to a law enforcement official and relevant Ministry or Agency

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 reason or cause of the occurrence of the failure in protecting the secrecy of Personal Data;
- can be conducted electronically, if the Personal Data Owner has given Consent for it, at the time of obtaining and collecting his / her 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
- a 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:

- IDR 600 million fine to IDR 800 million and six to eight years imprisonment for unlawful access
- IDR 800 million fine and / or 10 years imprisonment for interception or wiretapping of a transmission
• IDR 2 billion to IDR 5 billion and / or 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. 71 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;
• termination of access; and / or
• 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; and / or
• 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. 71 do not specifically address electronic marketing. Article 25 of the EIT Law provides that an Internet website, amongst 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
Ivan Almaida Baely & Firmansyah
T +62 21 5790 5090
erwin.purba@iab-net.com

Robert Hasan
Associate
Ivan Almaida Baely & Firmansyah
T +62 21 5790 5090
robert.hasan@iab-net.com

Fariz Ghassen
Associate
Ivan Almaida Baely & Firmansyah
T +62 21 5790 5090
fariz.ghassen@iab-net.com

Michael Pandjaitan
Associate
Ivan Almaida Baely & Firmansyah
T +62 21 5790 5090
michael.pandjaitan@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.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.