DATA PROTECTION LAWS OF THE WORLD

Indonesia

DLA PIPER

INDONESIA

Last modified 2 January 2024

LAW

Specific regulations

Indonesia has adopted an overarching framework for personal data protection through the enactment of Law No. 27 of 2022 concerning Personal Data Protection ("**PDP Law**") since 17 October 2022. Data controllers, data processors and relevant parties that process personal data are given a two (2) year transition period following the enactment of the PDP Law, thus up to 17 October 2024 to conform with the PDP Law. Once the transition period elapses, all such parties must comply with all the provisions of the PDP Law and any incompliance thereto may possibly be enforced.

The PDP Law is closely aligned with international data privacy standards, and is largely modelled on the European Union’s General Data Protection Regulation ("**GDPR**").

Before the enactment of the PDP Law, there was no comprehensive law on privacy / personal data protection in Indonesia. Instead, separate legislations which are embedded in and / or spread out in a number of sector specific (e.g. financial sector), matter specific (e.g. e-commerce), and / or nature specific (e.g. personal data processed in / through electronic systems) regulations regulate the general aspects of the protection of privacy / personal data were relied upon. Examples include the 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 and Law No. 1 of 2024 regarding the Second Amendment of EIT Law, Government Regulation No. 71 of 2019 regarding the Operation of Electronic Systems and Transactions ("**Reg. 71**") and its implementing regulations such as the Minister of Communications and Informatics Regulation No. 5 of 2020 regarding the Private Sector Electronic System Operator, as lastly amended by Minister of Communications and Informatics Regulation No. 10 of 2021 ("**MOCI Reg. 5/2020**"), and Minister of Communication & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System ("**MOCI Reg. 20/2016**"). These existing rules on privacy / personal data protection in the framework of processing personal data through electronic systems will be referred to as “General Data Protection Regulations”.

Other than provisions relating to data protection under General Data Protection Regulations, examples of sector specific regulations which also include provisions relating to data protection include the following:

Telecommunications sector

Article 40 of Law No. 36 of 1999 regarding Telecommunications ("**Telecommunications Law**") as partially amended by Law No. 11 of 2020 on Job Creation which was later revoked and replaced by Law No. 6 of 2023 on the Enactment into Law of Government Regulation in Lieu of Law No. 2 of 2022 on Job Creation (generally referred to as the "**Omnibus Law**") provides that any person is prohibited from any kind of tapping of information transmitted through any kind of telecommunications network. Article 42 paragraph (1) 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.[1]

Public information sector

Article 6 paragraph (3) point c of Law No. 14 of 2008 regarding Disclosure of Public Information ("**Public Information Law**")[2] provides that information relating to personal rights may not be disclosed by public bodies. Furthermore, Article 17 point (h) of the Public Information 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), evaluation records concerning a person's capability / recommendation / intellectual, and / or formal and informal education records.

Banking and capital market sectors

Data privacy in the banking sector is regulated under Law No. 7 of 1992 as amended by Law No. 10 of 1998 on Banking ("**Banking Law**") and as partially amended by the Omnibus Law and Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, including the implementing regulations. As regards the capital market sector, it is generally regulated under Law No. 8 of 1995 on Capital Market ("**Capital Market Law**”) which was partially revoked by Government Regulation In Lieu of Law No. 1 of 2017 on Access to Financial Information for Tax Purposes and amended by Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, including the implementing regulations. The regulations mentioned above apply to both individuals and corporate data[3].

Principally, commercial banks' customer data transfer (by way of establishing a data center or a data processing outside Indonesia territory) necessitates prior approval being obtained from the Indonesian Financial Services Authority ("**FSA**")[4].

Generally, those separate sector specific legislations will principally still be valid so long they do not contradict with the PDP Law. It is anticipated that further implementing regulations will be drawn up and issued (which may or may not revoke existing legislations on the protection of privacy / personal data), and a separate institution / agency will be formed to specifically handle and undertake the organization of the protection of privacy / personal data in accordance with the PDP Law ("**PDP Agency**").

In the meantime, the first draft of Government Regulation on the Implementation of the PDP Law ("**Draft Implementing Regulation to PDP Law**") has been circulated for public comments from August 31st, 2023 until September 25th, 2023. The drafting process was targeted to be concluded at the end of 2023, however, it seems that the legislator is still in the process of identifying and analysing a total of 1,989 input to the Draft Implementing Regulation to PDP Law, as announced through a dedicated website that is accessible at pdp.id.

1: Please note that the Omnibus Law only partially amended the Telecommunications Law, thus Articles 40 and 42 of the Telecommunications Law are still valid and fully enforced.

2: Please note that Law No. 14 of 2008 regarding Disclosure of Public Information has been partially amended with Constitutional Court Judgement Number 77 / PUU-XIV / 2016, however Articles 6 and 17 of Law No. 14 of 2008 regarding Disclosure of Public Information have not been amended.

3: Please note that the Omnibus Law does not amend the Articles that governs data protection in Banking Law.

4: Please note that Article 35 paragraph (3) of the Financial Services Authority Regulation No. 11/POJK.03/2022 on the Organization of Information Technology by Commercial Banks necessitates commercial banks to obtain prior approval from the FSA in the event such commercial banks intend to establish a data center or a data processing outside Indonesia territory.

DEFINITIONS

Definition of personal data

Personal data under the General Data Protection Regulations and the PDP Law is broadly defined as any data of an individual who can be identified and / or may be identified individually or combined with other information both directly or indirectly through

electronic or non-electronic systems.

Definition of sensitive personal data

Sensitive personal data under the PDP Law is referred to as "specific personal data", which would include any (i) health data and records, (ii) biometric data, (iii) genetic data, (iv) sexual life / orientation, (v) political views, (vi) criminal records, (vii) children’s data, (viii) personal financial data, and / or (ix) any other data as (may be) provided in accordance to the prevailing laws and regulations. There is however, no clear / specific differentiation between the requirements for processing of general and specific personal data, except that:

- a data controller may be obligated to carry out a data protection impact assessment when processing personal data with a high potential risk to data subjects, which includes, among others, such an event where it would process specific personal data;
- a personal data controller and processor may be obliged to appoint a data protection officer (DPO), in the event that the main activity of the personal data controller consists of processing personal data in a large scale that involves specific personal data and / or that relates to criminal acts. Further provisions may possibly be set out in subsequent implementing regulations to the PDP Law.

NATIONAL DATA PROTECTION AUTHORITY

Under the PDP Law, a separate institution / agency (the PDP Agency mentioned earlier) will be formed to specifically handle and undertake the organization of the protection of privacy / personal data, whom will be tasked, among others, to formulate policies / strategies, to supervise / monitor the implementation of the PDP Law, to enforce administrative sanctions for non-compliance with the PDP Law, and to facilitate non-court dispute settlements. A presidential regulation would be issued in respect to such a PDP Agency, while procedures to implement the authorities of the PDP Agency will be set out in a government regulation, both which as of writing are yet to be issued.

During the two (2) year transition period of the PDP Law and until such a PDP Agency is formed and operating, the Ministry of Communications and Informatics of the Republic of Indonesia ("**MOCI**") will largely still have the authority over data privacy matters that are processed through electronic systems in accordance to the General Data Protection Regulations.

However, it does not rule out the possible enforcement by:

- other relevant sector’s regulatory authority (in the event the data controller / processor is subject to a regulated sector) which may also impose certain other administrative sanctions; for example, the FSA has the authority to act as the regulator of data privacy in the capital market sector (since 31 December 2012) and with regard to banks’ customer data privacy issues (since 31 December 2013); or
- the law enforcement agency (prosecutor) if non-compliance involves a criminal offense, which may subject the accused to imprisonment and / or fines.

REGISTRATION

The PDP Law does not contain a specific obligation to register and / or notify supervisory authorities of the processing of personal data.

However, it is to be noted that there is a general registration obligation with the MOCI for any foreign and / or Indonesian party, who provides, manages, and / or trades goods and / or services through electronic systems and / or over the internet as an electronic system operator, provided that:

- it provides services in the territory of Indonesia;
- it conducts business in Indonesia; and / or
- its electronic system is used and / or offered in the territory of Indonesia.

Such a party (commonly also referred to as a "electronic system operator" or "**PSE**") would be required to make certain registration with the MOCI before its electronic system is to be used in Indonesia which will be marked by the grant of an

electronic system operator registration certificate (*Surat Tanda Terdaftar Penyelenggara Sistem Elektronik* or commonly abbreviated as "**TDPSE**").

Such a registration requirement is to ensure the reliability, security and compatibility of the electronic system in processing any personal data stored in it. Certain publication of the PSE’s profile is intended to and / or will be made on a website operated by the relevant authority (MOCI) upon successful registration.

DATA PROTECTION OFFICERS

There is no requirement in Indonesia for organizations to appoint a data protection officer except in certain situations mentioned below.

The PDP Law formally establishes the position of a data protection officer (DPO) into Indonesian law, which was nonexistent under the General Data Protection Regulations.

The PDP Law only requires data controllers and data processors to mandatorily appoint a data protection officer (DPO) in the event that:

- the personal data processing is for public service purposes;
- the main operations of the data controller require large-scale, frequent and systematic monitoring of personal data; or
- the main operations of the data controller involve large-scale personal data processing of specific personal data and / or personal data related to criminal activity.

This data protection officer (DPO) shall, at the very least, carry out the functions of:

- informing and providing advice to data controllers or data processors regarding compliance with the PDP Law;
- monitoring and ensuring compliance with the PDP Law and the internal policies of a data controller or data processor;
- providing advice regarding the personal data protection impact assessment and monitoring the performance of data controllers or data processors; and
- coordinating and acting as a contact person for issues related to personal data processing.

Further conditions on DPOs will be set out in separate a government regulation, which as of writing hereof is yet to be issued.

COLLECTION & PROCESSING

Based on the PDP Law, processing of personal data includes:

1. obtainment and collection;
2. processing and analyzing;
3. storing;
4. correction and updates;
5. displaying, announcing, transferring / transmitting, distributing or disclosure / providing access to; and / or
6. deletion or removal.

With the enactment of the PDP Law, the lawfulness of processing personal data has been extended and is largely similar with the GDPR, which are currently as follows:

- **consent**: the data subject has given explicit consent to the processing of his / her personal data for one or more specific purposes as have been conveyed by the data controller to the data subject;
- **contractual obligation**: processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject upon entering into a contract;
- **legal obligation**: processing is necessary for compliance with a legal obligation to which the controller is subject to;
- **vital interest**: processing is necessary in order to protect the vital interests of the data subject ("vital interest of the data subject" relates to the survival of the data subject such as when the processing is necessary for serious medical treatment proceedings);
- **public interest**: processing is necessary for the performance of a task carried out in the public interest, public service or

the exercise of official authority vested in the data controller in accordance to prevailing laws and regulations; and / or

- **legitimate interest**: processing is necessary for the purposes of other legitimate interests with due regard to the purpose, needs and balance of interest of rights of the data controller and the data subject.

The current Draft Implementing Regulation to PDP Law (version of August 31st, 2023) suggests some further guidance containing the criteria and / or restrictions in regard to each lawful basis.

The PDP Law also re-emphasizes the principles of personal data protection that are also set out in the General Data Protection Regulations, which includes:

- personal data collection is conducted in a limited and specific manner, legally valid, fairly, with the knowledge and approval of the personal data owner (transparency);
- 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;
- 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; and
- processing of personal data shall be carried out responsibly and shall be verifiable in a clear manner.

TRANSFER

Cross border transfers

Transfers of personal data, including transfers outside of the territory of the Republic of Indonesia would principally require an underlying basis. Cross border transfers are principally permitted provided that, the transferring data controller is able to ensure the following:

- that the country of domicile of the data controller or data processor that will receive the transfer of personal data has an equal or higher level of personal data protection than afforded under the PDP Law ("**Adequacy of Protection**");
- in the absence of Adequacy of Protection, an adequate level of binding personal data protection shall be available ("**Appropriate Safeguards**");
- in the event that neither Adequacy of Protection nor Appropriate Safeguards are present, (prior) consent shall be obtained from the data subject.

Further terms in connection hereof, is intended to be set out in a government regulation, which as of writing hereof is yet to be issued.

The current Draft Implementing Regulation to PDP Law (version of August 31st, 2023) suggests that such Adequacy of Protection assessment will be made by the PDP Agency (which as of the date hereof is yet to be formed and operating), whom consequently may issue a list of such countries that have equal / higher level of personal data protection.In practice and for the time being, the absence of a PDP Agency as well as relevant implementing regulations to the PDP Law, implies that the General Data Protection Regulations will largely still apply, which would subject a data exporter / transferor with the obligations to:

- ensure the effectiveness of supervision by the relevant governmental institutions and law enforcer. Data exporter / transferor is obliged to provide access to its electronic system and electronic data if required in the framework of supervision and law enforcement pursuant to the prevailing laws and regulations. In practice this would imply that the data exporter / transferor shall also ensure that the country in which its electronic system and electronic data is being managed, processed and / or stored, has cooperative and / or diplomatic relations with the Republic of Indonesia, to allow relevant Indonesian government institutions and / or law enforcers to obtain access to any such required electronic system and electronic data; and

- prior to such transfer, coordinate with the Directorate General for Informatics Application (*Direktorat Jenderal Aplikasi Informatika* or commonly abbreviated as "**DITJEN APTIKA**") within the MOCI. This implies the obligation of the personal data exporter / transferor to make and submit certain reports to DITJEN APTIKA.

SECURITY

The PDP Law does not provide specific technical standards or measures. It, however, does provide certain general measures to data controllers, who are obliged to protect and ensure the security of personal data that it processes, by requiring them to:

- set out and implement operational technical measures to protect personal data from any disruption in the processing of personal data that is contrary to the provisions of laws and regulations; and
- determine the appropriate level of security of the personal data by taking into account the nature and risk of personal data which must be protected in the processing of personal data.

Whilst anticipating the issuance of further implementing regulations to the PDP Law, certain fundaments to ensuring the security of personal data may be found in the General Data Protection Regulations, which sets out certain obligations to electronic system operators (PSEs) in particular. The obligations of such PSEs are regulated under Reg. 71 and MOCI Reg. 20/2016, whom 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 implements;
- 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 sector PSEs 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.

An online self-assessment on the security system’s risk level and compliance is since recently also offered upon the application for an electronic system operator registration certificate (TDPSE). Although it is a self-assessment, the feature is to a certain degree mandatory, as an applicant for TDPSE may not be able to proceed in submitting its application before it fills out certain part of the online self-assessment about its security system’s risk level and compliance.

In the telecommunications sector, Article 19 paragraph (2) of Minister of Communication and Informatics Regulation No. 26/PER/M.KOMINFO/5/2007 regarding the Security and Utilization of Internet Protocol based Telecommunications Network (as amended) ("**MOCI Reg. 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 3 months.

BREACH NOTIFICATION

The PDP Law contains a general requirement for a personal data breach to be notified by the controller to both (i) the affected

personal data subjects and (ii) the PDP Agency, and for more serious breaches which would disturb public services and / or significantly affect the public interest, to also be notified to the public.

Personal data breach is a wide concept, which under the PDP Law is referred to as a "personal data protection failure" and defined as any "failure in protecting a person’s personal data in terms of confidentiality, integrity, and availability of the personal data, including security breaches, whether intentional or unintentional, which lead to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed".

The PDP Law stipulates that in the event of such a personal data protection failure, the personal data controller must deliver a written notification within 72 hours.

The PDP Law provides guidelines on the required content of the written notification, which must at least include:

- a description of the personal data that was breached;
- when and how the personal data was breached; and
- the efforts undertaken by the personal data controller to mitigate the effects of the data breach and recover affected personal data.

However, during the transition period of the PDP Law and until the PDP Agency is formed and operating, data breach notifications should continue to be submitted to the MOCI and other relevant institution(s) pursuant to General Data Protection Regulations, which includes the following terms:

A. Reporting obligations to relevant authorities:

- if there is a serious system interference or failure caused by acts of a third party on its electronic system, a report shall be made immediately and at a first instance to:
    - a law enforcement official (in practice, mostly if the breach is suspected to contain matters related to cybercrimes); and
    - relevant Ministry or Agency (namely DITJEN APTIKA, and if required (often also as a matter of custom / courtesy) its specific sector’s authority.

  However, there is no specific definition or elucidation provided on what "immediately" or "first instance" shall mean. In practice, typically, such an event would be reportable if there is certain loss, namely where the impact due to failure of the electronic system has legal consequence to the user, operator and other parties, both material and immaterial.

- on the content / coverage of the report, there is no specific minimum information prescribed, except that the electronic system operator / PSE (data controller / processor), shall also take the necessary measures to secure the electronic information / document under its control.

  However, in practice and pursuant to the DITJEN APTIKA’s current policy, DITJEN APTIKA has made available a prescribed notification format which shall be completed with, among others, the following information:

- How the notifying party is aware of such breach;
- Description of the event;
- Period of the incident;
- Category of the disclosed personal data (general data and / or specific data);
- Estimation of the total affected individuals;
- The affected person’s status (employee, consumer, student and etc);
- Description of the interfered components of the electronic system;
- Impact to the notifying party;
- Period of recovery (for the notifying party to recover the electronic system);
- Accessibility of data protection trainings for the individuals involved in the processing of personal data of the notifying party;
- Efforts to handle and recover from the disclosure of personal data by the personal data controller;
- Efforts to prevent future issues; and

- Notification to the affected individuals

B. Notification obligations to relevant data subject:

- a notification shall be sent within 14 (calendar) days as of discovery / determination of a breach, namely upon failure to protect the secrecy of the personal data in the electronic system.

There is no further description on what would contain a "failure to protect the secrecy of the personal data". The MOCI would as a general rule consider such a failure present, in the event that other parties (with no rights to access) may identify the affected person based on the disclosed data.

- on the content / coverage of the notification, it must at the minimum provide the reason or cause of the occurrence of the failure in protecting the secrecy of personal data. No specific format is prescribed.

ENFORCEMENT

Sanctions

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.

Enforcement by the PDP Agency (administrative sanctions)

Violations of certain articles in the PDP Law are subject to administrative sanctions. These administrative sanctions, which shall be imposed by the PDP Agency, are as follows:

- written warning;
- temporary suspension of personal data processing activities;
- deletion or destruction of personal data; and / or
- administrative fines.

With regard to administrative fines, the PDP Law stipulates that the maximum fine is 2% of the concerned party's annual income or revenue. Further provisions on administrative sanctions and the procedures for the imposition of administrative fines will be provided in Government Regulations.

Enforcement by the public prosecutor (criminal sanctions)

- Every person is prohibited from unlawfully obtaining or collecting personal data not belonging to themselves, and with the intention of benefiting themselves or another person which may result in the loss for the data subject. Violation of this is subject to maximum imprisonment of five (5) years and / or a maximum fine of IDR 5 billion (±USD334,000);
- Every person is prohibited from unlawfully disclosing personal data that does not belong to themselves. Violation of this is subject to maximum imprisonment of four (4) years and / or a maximum fine of IDR 4 billion (±USD267,000);
- Every person is prohibited from using personal data that does not belong to such person in a manner that contravenes the law. Violation of this is subject to maximum imprisonment of five (5) years and / or a maximum fine of IDR 5 billion (±USD334,000);
- Every person is prohibited from creating false personal data or fake personal data with the intention of benefiting themselves or other persons that may cause harm to other persons. Violation of this is subject to maximum imprisonment of six (6) years and / or a maximum fine of IDR 6 billion (±USD400,000).

Additional penalties may also be imposed in the form of confiscation of profits and / or assets obtained or proceeds from criminal acts and indemnity payment.

If the criminal act is committed by a corporate entity, the PDP Law stipulates that criminal sanctions will be imposed only in the form of criminal fines. These fines will be imposed on the management, controller, instructor, beneficial owner, and / or the corporation itself. The administrative fines for corporate entities can be up to 10 times the maximum fines for individuals.

Additional criminal sanctions that may be imposed on corporate entities, include:

- confiscation of profits and / or assets obtained or proceeds from criminal acts;
- suspension of all or part of the business of the corporation;
- permanent prohibition on certain activities;
- closure of all or part of the business premises and / or activities of the corporation;
- fulfilment of the neglected obligation;
- payment of compensation;
- revocation of licenses; and / or
- dissolution of the corporation.

Since the above provisions relate to prohibited conducts related to personal data that shall be enforced by the public prosecutor, these would already have effect since the enactment of the PDP Law.

Enforcement by the MOCI (administrative sanctions)

Considering that there is no specific data protection authority yet formed and operating (which with the recent enactment of the PDP Law is intended to be assumed by the PDP Agency), therefore, reference hereinbelow would still apply, and it is currently still the MOCI that is responsible for monitoring and regulating data protection (in the context of personal data in electronic systems).

The MOCI has the right to request data and information from the electronic system operator (data controller / processor) for the purpose of protecting personal data.

It may also enforce non-complying parties by imposing administrative sanctions in the form of:

- written warnings;
- temporary restriction / suspension of its business activities;
- administrative fines (in coordination with the relevant sector’s regulatory authority). The regulation does not specify the amount of administrative fines or the procedure to impose such fines;
- restriction to the access of the electronic system and/or information / data; and / or
- the business actor being excluded from certain registration list, and / or
- online publication in the website.

The ultimate sanction in MOCI Reg. 5/2020 is the blocking of access to the private electronic system operator’s (PSE’s) electronic systems in Indonesia. Access can be granted again once the private PSE has fulfilled its obligations.

However, as mentioned earlier, it does not rule out the possible enforcement by:

- other relevant sector’s regulatory authority (in the event the data controller / processor is subject to a regulated sector) which may also impose certain other administrative sanctions; and / or
- the law enforcement agency (prosecutor) if the non-compliance implies a criminal offense, which may subject the accused with imprisonment and / or fines.

Banking Law

Under Article 47 paragraph (2) of the Banking Law, any commissioner, director or employee of a bank or its affiliates who intentionally provides information which has to be kept confidential may be sentenced to imprisonment for not less than two (2) years but not more than four (4) years, and fined at least IDR 4 billion (±USD267,000) but not more than IDR 8 billion (±USD534,000).

Capital Market Law

Under the Capital Market Law, the FSA 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; and / or
- Cancellation of registration.

Right to file a complaint

The PDP Law provides personal data subjects with the right to file a complaint against automated decision making.

Under the General Data Protection Regulations, an affected individual has the right to file a civil claim to the relevant electronic system operator (data controller / data processor) for losses incurred. On the other hand, it is also provided with the right to make complaints related to data protection infringements to the Directorate General for Informatics Application (*Direktorat Jenderal Aplikasi Informatika* or commonly abbreviated as "**DITJEN APTIKA**") within the MOCI in the event that there has been:

- no written notification made by the electronic system operator (data controller / processor) to the data subject concerning a data breach; or
- losses have been incurred by the data subject due to a data breach.

In addition, the general right to file a complaint is embedded in the Indonesian Civil Code, which provides that any party may claim for civil liability if any loss suffered may be evidenced to be resulting due to another party’s unlawful act.

ELECTRONIC MARKETING

The PDP Law and the General Data Protection Regulations do not specifically address electronic marketing.

Similar with other processing activities of personal data, a legal basis shall be available for conducting (electronic) marketing activities, (e.g. consent of the personal data subject).

It is interesting to note that one of the reasons for the introduction of the right to withdraw consent under the PDP Law was to enable personal data subjects to avoid (further) personal data breach occurrences which have emerged due to, among others, direct marketing practices.

ONLINE PRIVACY

There are currently no laws and regulations concerning cookies and location data.

Insofar the data generated through cookies or other tracking technologies, do not contain personal data, the use of thereof is generally permitted. Conversely, if any such cookies or tracking technologies do collect / generate personal data, then the use thereof shall be subject to the prevailing laws and regulations on personal data protection.

KEY CONTACTS

Tumbuan & Partners

Jennifer B. Tumbuan
Senior Partner
Tumbuan & Partners
jennifer.tumbuan@tumbuanpartners.com

Lingkan S. Ngantung
Partner
Tumbuan & Partners
lingkan.ngantung@tumbuanpartners.com

DATA PRIVACY TOOL

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