DATA PROTECTION & PRIVACY

Indonesia

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 05 August 2022

Table of contents

Contributors

Indonesia

Rusmaini Lenggogeni
rusmainilenggogeni@ssek.com
SSEK Legal Consultants

Charvia Tjhai
charviatjhai@ssek.com
SSEK Legal Consultants

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Indonesia has yet to enact a data protection regulation that would apply to PI. To date, Indonesia does not have in place a single and comprehensive law governing data privacy or data protection. The relevant provisions on the protection of privacy of PI are spread across various laws and regulations, namely:

- Law No. 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law No. 19 of 2016 (25 November 2016) (the Electronic Information Law);
- Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019);
- Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016); and
- MOCI Regulation No. 5 of 2020 regarding Private Electronic Systems Providers (24 November 2020), as amended by Law No. 10 of 2021 (21 May 2021) (MOCI Regulation 5/2020).

The above laws and regulations are hereinafter collectively referred to as the PDP Regulations.

It is important to note that the government is preparing a Personal Data Protection Draft Bill (the PDP Draft Bill), which would recognise standard international concepts such as data controller, data processor, sensitive personal data, dedicated data protection officers and automatic processing once the PDP Draft Bill is enacted. As of the time of writing, however, the PDP Draft Bill has not been passed and is still being discussed at the House of Representatives. It was reported that the PDP Draft Bill was targeted for enactment by 2022.

Other than the above PDP Regulations, the protection of personal data is included in several sector-specific laws and regulations, though most of these laws and regulations only address data protection briefly. These are:

- Law No. 36 of 2009 regarding Health (13 October 2009), which stipulates that, in principle, every person is entitled to the confidentiality of their personal health information that has been provided to or collected by healthcare providers (the Health Law);
- Bank Indonesia Regulation No. 22/20/PBI/2020 regarding Bank Indonesia Consumer Protection (22 December 2020);
- Financial Services Authority (OJK) Regulation No. 1/POJK07/2013 regarding Financial Consumer Protection (6 August 2013), as last amended by OJK Regulation No. 18/POJK07/2018 (10 September 2018) (OJK Regulation 1/2013). OJK Regulation 1/2013 prohibits financial service providers from disclosing customer data or information to third parties without written consent from the customer or unless they are required to make such disclosure by law. Where a financial service provider obtains the data or personal information of a person or a group of persons from a third party, it is required to obtain written confirmation from the third party that the person or group of persons has agreed to the disclosure; and
- Law No. 36 of 1999 regarding Telecommunications (8 September 1999), which prohibits the tapping of information transmitted through telecommunications networks. Telecommunications service operators must maintain the confidentiality of any information transmitted or received by a telecommunications subscriber

through a telecommunications network or telecommunications service provided by the respective operator.

Law stated - 20 May 2022

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

To date, there is no specific data protection authority that oversees data protection in Indonesia. Under the PDP Regulations, the MOCI is responsible for monitoring and regulating data protection.

To the extent of its investigative power, the MOCI also has the power to, among other things, organise and supervise information related to the transfer of personal data or impose administrative sanctions for violations of data protection regulations. However, for specific matters, such as a dispute related to the failure or breach of personal data protection, data subjects may submit a written complaint to the Directorate General of Application of Informatics (DGAI), part of the MOCI, within 30 business days from the discovery of the failure to protect the personal data of the data subject. If a violation is found, the DGAI may recommend that the MOCI impose certain administrative sanctions on the Electronic System Provider (ESP).

Also, certain other government agencies may oversee data protection for their respective sectors, such as the OJK for financial service providers and the Ministry of Health for healthcare providers.

Law stated - 20 May 2022

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

In general, the MOCI may cooperate with other data protection authorities, such as other governmental agencies, to follow up on complaints from data subjects regarding the failure to protect personal data. However, the MOCI has not entered into any cooperation agreements with foreign authorities.

Law stated - 20 May 2022

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Each of the PDP Regulations stipulates different sanctions. The Electronic Information Law regulates criminal sanctions, while GR 71/2019 and MOCI Regulation 20/2016 only stipulate administrative sanctions. The administrative sanctions under GR 71/2019 and MOCI Regulation 20/2016 also differ. Nonetheless, the following sanctions stipulated thereunder are equally enforceable by the MOCI:

- MOCI Regulation 20/2016 imposes administrative sanctions for breaches of data protection in the form of:
  - a verbal warning;
  - a written warning;
  - a temporary suspension of activities; or
  - an announcement on the MOCI website; and

- GR 71/2019 imposes administrative sanctions due to breaches of data protection in the form of:
  - a written warning;
  - an administrative penalty;
  - a temporary suspension of activities;
  - termination of access to the electronic system; or
  - the expulsion from the list of registered ESPs for the violation of certain provisions of GR 71/2019 relating to the protection of personal data.

If applicable, the imposition of the above administrative sanctions does not eliminate criminal and civil responsibilities.

Criminal sanctions, which can be imposed on both corporations and individuals, may also apply as follows:

- fines of 600 million rupiah to 800 million rupiah or four to eight years' imprisonment for unlawful access;
- fines of 800 million rupiah to 1 billion rupiah or six to 10 years' imprisonment for interception or wiretapping of a transmission;
- fines of 2 billion rupiah to 5 billion rupiah or eight to 10 years' imprisonment for the alteration, addition, reduction, transmission, tampering, deletion, moving or hiding of electronic information or electronic records; and
- fines of 10 billion rupiah to 12 billion rupiah or 10 to 12 years' imprisonment for the manipulation, creation, alteration, destruction, or damage of electronic information or electronic documents with a purpose of creating an assumption that such electronic information or documents are authentic, and other violations related to the processing of electronic information or documents.

Criminal proceedings are initiated by the Indonesian police and prosecutors.

Law stated - 20 May 2022

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

In general, the PDP Regulations do not provide specific rules for appeal to the courts against orders of the data protection authority. However, according to the PDP Regulations, in general, PI owners have the right to file a lawsuit or claim for damages if their rights related to PI under the relevant laws and regulation are infringed.

Law stated - 20 May 2022

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The current PDP Regulations are rather broad, as can be seen from the definition of an Electronic System Provider (ESP). An ESP is defined as every person, state administrator, business entity and community providing, managing, or operating an electronic system, either individually or jointly, for electronic system users, for their personal purpose or another party's purpose. The term 'electronic system' is defined as a set of electronic devices and procedures that function to prepare, collect, process, analyse, retain, display, publish, transmit or disseminate electronic information. The Minister of Communication and Informatics (MOCI) has interpreted this to mean that any person or entity that

stores data electronically is considered an ESP using an electronic system that should be subject to the PDP Regulations.

ESPs are further divided between private scope ESPs and public scope ESPs, as further defined below:

- private scope ESPs: MOCI Regulation No. 5 of 2020 regarding Private Electronic Systems Providers (24 November 2020), as amended by Law No. 10 of 2021 (21 May 2021), defines private scope ESPs as individuals, business entities and communities that provide electronic systems; and
- public scope ESPs: GR 71/2019 defines public scope ESPs as state administrative agencies, legislative, executive and judicial institutions at the central and regional government level and other agencies that are formed by virtue of laws and regulations, and institutions appointed by state administrative agencies. The latter refers to institutions providing an electronic system with a public scope on behalf of the appointing state administrative agency.

GR 71/2019 excludes public scope ESPs that have regulatory and supervisory authority in the financial sector.

Law stated - 20 May 2022

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

First, an interception of communication is generally governed by Law No. 11 of 2008 regarding Electronic Information and Transactions (21 April 2008), as amended by Law No. 19 of 2016 (25 November 2016) (the Electronic Information Law), which stipulates that any interception or wiretapping of a transmission shall be subject to criminal sanction in the form of a maximum fine of 800 rupiah million and up to 10 years' imprisonment. However, exemptions apply for lawful interception or wiretapping of a transmission in the framework of law enforcement, such as in a corruption case investigation.

Second, concerning electronic marketing or monitoring and surveillance of individuals, if such action is conducted using electronic means, then it must comply with personal data protection principles and relevant rules under the PDP Regulations.

Law stated - 20 May 2022

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

The PDP Regulations do not regulate this matter. We are also not aware of any specific regulations on employee monitoring. In this regard, considering that the concept of employee monitoring is not recognised under the PDP Regulations or any other Indonesian laws or regulations, and to the extent the employer qualifies as an ESP and processes the personal data of employees, who may be considered data subjects, consent is required.

For e-health records, Law No. 36 of 2009 regarding Health (13 October 2009) stipulates that, in principle, every person is entitled to the confidentiality of their personal health information that has been provided to or collected by healthcare providers. This personal health information shall be considered personal data. Concerning the use of social media, it shall also be subject to the data protection requirements under the PDP Regulations as they pertain to user consent for

the collection and processing of personal data.

Last, credit card information is considered confidential information in the banking sector. Financial Services Authority (OJK) Regulation No. 1/POJK07/2013 regarding Financial Consumer Protection (6 August 2013), as last amended by OJK Regulation No. 18/POJK07/2018 (10 September 2018) (OJK Regulation 1/2013), prohibits financial service providers from disclosing customer data or information to third parties unless they receive written consent from the customer or are required to make such disclosure by law.

Law stated - 20 May 2022

PI formats

What categories and types of PI are covered by the law?

The definition of personal data has evolved throughout the enactment of the PDP Regulations. MOCI Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) defines personal data as certain personal data that is stored or cultivated, with its accuracy maintained and confidentiality protected. GR 71/2019 further defines personal data as any data relating to a person that is identified or is self-identifiable, or is combined with other information, directly or indirectly, through electronic and non-electronic systems. The current regulatory framework does not elaborate or explain one's identifiability threshold. Further, concerning the format, it shall apply only to personal data processed by electronic means under the PDP Regulations.

Law stated - 20 May 2022

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

Article 2 of the Electronic Information Law provides that it has an extraterritorial scope if the actions of individuals outside of Indonesia have a legal implication within the territory of Indonesia or if they adversely affect Indonesian interests. On a plain reading of the above provision, the Electronic Information Law may apply to breaches of personal data outside of Indonesia to the extent the effect concerns the personal data of Indonesian data subjects. However, we have not seen the government apply the PDP Regulations to entities outside of Indonesia.

Law stated - 20 May 2022

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The PDP Regulations define an ESP as a person, state administrator, business entity, or community that provides, manages, or operates an electronic system, individually or jointly, to or for electronic system users for their own or another party's benefit. The PDP Regulations do not recognise the concept of the processor. The PDP Regulations instead refer to an ESP as the party controlling and managing the use of personal data. Unlike controllers, the PDP Regulations do not refer to processors. Further, the PDP Regulations do not define data processors or distinguish them from data controllers. Therefore, we understand that the term 'data controllers' primarily refers to ESPs.

Law stated - 20 May 2022

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The PDP Regulations mandate the obtainment of consent for any processing of personal data. However, the PDP Regulations do not provide further guidance on how this consent is to be given.

In addition to consent, Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) stipulates lawful bases other than consent for processing personal data, which are:

- processing an individual's personal data to satisfy the obligations of a contract or to fulfil the request of such personal data owner when agreeing;
- the fulfilment of the legal obligation of the personal data controller in line with the applicable laws and regulations;
- guarding the vital interest of the personal data owner;
- performing the legal obligation of the personal data controller;
- performing the obligation of a public service personal data controller in the interest of the public; and
- satisfying another valid interest of the personal data controller or the personal data owner.

The wording in the relevant clause regarding lawful bases is rather ambiguous and may be interpreted to mean that consent is still required despite the existence of these lawful bases.

Further, under GR 71/2019, consent can only be considered lawful if it fulfils the following conditions:

- explicitly given, apparent and not hidden;
- shall not be based on fault, negligence or duress;
- for one or more specific purposes; and
- for the informed purposes.

Law stated - 20 May 2022

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

Indonesia recognises that all information is personal data and shall receive the same processing and protection.

However, we understand that more stringent rules may apply in specific cases or circumstances (eg, in the financial services sector). Under OJK Circular Letter No. 14/SEOJK07/2014 on the Confidentiality and Security of the Personal Data or Information of Consumers, personal data consisting of name, address, birth date or age, phone number or the subject's biological mother's name can only be shared with a third party with the consent of the personal data owner or as is obligated by laws and regulations.

Law stated - 20 May 2022

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The PDP Regulations recognise the term transparency. For example, electronic system providers (ESPs) must notify data subjects of data breaches within 14 days of the discovery of a breach. In such regard, by nature, an ESP, acting as the controller of data, shall notify the individuals of the processing activities.

In particular for consent, although the PDP Regulations do not provide further guidance on how this consent is to be given, Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) and Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016) do provide more clarity on how the required consent is to be given.

MOCI Regulation 20/2016 defines 'consent' as:

For consent, specifically, the following rules apply:

- consent must be obtained by any ESP that processes (including any acquisition and collection, processing and analysing, storage, repairs and updates, appearance, announcement, transfer, dissemination, disclosure or deletion or destruction) personal data;
- the consent may be given only after the owner of the personal data confirms the veracity, confidentiality or non-confidentiality, and purpose of the personal data; and
- the consent must be given in the Indonesian language, but there is no prohibition against the consent including a second language (eg, a bilingual Indonesian and English form).

In practice, ESPs will require consent to be both broad and as specific as possible, covering, among other things, transfer of the collected data to a foreign server via the internet and transfer of the collected data to a foreign server after the collected data has been stored in Indonesia if these actions are intended.

That being said, in practice, the notification usually covers the collected information, processing purposes and activities, lawful basis of processing activities, the possibility to share or transfer collected information, access to collected information, contact details of the ESP, and so on.

Law stated - 20 May 2022

Exemptions from transparency obligations

When is notice not required?

In general, the PDP Regulations do not provide conditions that may exempt ESPs from the notice requirement. In practice, it is uncommon for an ESP that acts as a service provider to notify the data subject after being contracted by the ESP that initially collected the data. By nature, such notifications may be considered to be given by the initial ESP through the notice of processing.

Law stated - 20 May 2022

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

MOCI Regulation 20/2016 provides that one of the key forms of personal data protection is that the processing of personal data must be under the original purpose of its processing. GR 71/2019 also provides that ESPs must disclose to the data subjects the purpose of their processing of the personal data. That being said, an ESP is obligated to maintain the accuracy of PI from collection to its deletion.

Law stated - 20 May 2022

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The PDP Regulations recognise the general restrictions for collecting PI: the PI collected must be relevant, in accordance with the purpose of the collection and implemented accurately. Although not yet been implemented, we note that the PDP Draft Bill recognises that PI that may be collected must be restricted and specific, legal, proper and transparent. The PDP Regulations and PDP Draft Bill do not provide details of the type of PI that must be restrictively collected.

Law stated - 20 May 2022

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Data stored within an electronic system may be destroyed only after:

- the lapse of the regulatory data retention period under MOCI Regulation 20/2016 or any other regulation issued by the relevant authority; or
- upon the request of the data subject, unless otherwise governed under laws and regulations.

MOCI Regulation 20/2016 provides that ESPs must retain personal data for a minimum of five years unless stipulated otherwise by sectoral regulations. Data may be retained beyond the five-year period if it is to be used following its initial purpose.

Consent is also required for the deletion of data (which is considered a part of data processing). In practice, the form of consent that data subjects are required to provide to ESPs is worded as broad as possible to cover all types of data processing.

Law stated - 20 May 2022

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

MOCI Regulation 20/2016 provides that ESPs may only use the personal data of data subjects following the needs of the data subjects. Further, ESPs shall also ensure that the processing of the personal data shall be in line with the specific purpose that has been consented to by the data subject. Further, MOCI Regulation 20/2016 provides that one of the key forms of personal data protection is that the processing of personal data must follow the original purpose of its processing. The current regulatory framework does not specifically regulate the application of this restriction, including with respect to circumstances where an organisation would like to use PI for a new purpose.

GR 71/2019 provides that ESPs must disclose the purpose of their processing of personal data to the data subjects, which in some jurisdictions is referred to as the 'finality principle'. Further, MOCI Regulation 20/2016 provides that one of the key forms of personal data protection is that the processing of personal data must follow the original purpose of its processing.

The current regulatory framework does not specifically regulate some types of leniency in the form of compatible processing or purposes.

Law stated - 20 May 2022

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There are no express rules for automated decision-making. However, according to the PDP Regulations, unless provided otherwise by the laws and regulations, the use of any information through electronic media that involves the personal data of a person must be made with the consent of the person concerned. Any person whose rights are infringed may claim damages under this law.

Law stated - 20 May 2022

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The PDP Regulations provide that electronic system providers (ESPs) must keep data secure. Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) affirms this obligation and further provides that ESPs must have security procedures and infrastructure in place to prevent disruptions, failures and damage within electronic systems. GR 71/2019 does not go into further detail as to the minimum measures required for such security procedures and infrastructure, and to date this has not been regulated.

Law stated - 20 May 2022

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

In general, the PDP Regulations do not obligate ESPs to notify either the Minister of Communication and Informatics (MOCI) of a data breach, except for 'serious data breaches caused by third parties', as provided by GR 71/2019. Neither GR 71/2019 nor the PDP Regulations provide further guidance on how the above phrase is defined. However, based on our informal discussions with officials from the MOCI, the MOCI expects to be notified of any data breach.

While there is no expressed definition of data breach, the PDP Regulations recognise data breach as a situation where an ESP fails to protect obtained data and the data is used without the consent of the owner. In this regard, in the event of a data breach, ESPs must notify data subjects within 14 days of the discovery of the breach. In such regard, by nature, an ESP, acting as the controller of data, must notify the individuals of the processing activities.

In addition to the above, for data breach notification, under article 28(c) of Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation No. 20/2016), an ESP is required to deliver written notification to personal data owners if there is a failure to protect the confidentiality of personal data within the electronic system managed by the ESP. This written notification must be made in line with the following terms:

- accompanied by the reason or cause for the failure to protect such confidentiality;
- can be done electronically if the personal data owner has consented to such method of notification during the obtainment and collection of his or her personal data;
- must be ensured to have been received by the personal data owner if such failure of confidentiality has the potential to cause damages to those involved; and
- the written notification must be delivered to the personal data owner at the latest 14 days since knowledge of such failure.

If an ESP does not adhere to the above terms it may be subject to sanctions under MOCI Regulation 20/2016. Further, failure to provide timely written notification gives affected personal data owners the opportunity to submit a complaint to the MOCI, irrespective of whether such failure has any potential to cause damages.

Law stated - 20 May 2022

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Pursuant to Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016), electronic system providers (ESPs) are required to have internal documentation for the purpose of personal data protection. This is basically internal rules or policies for the management of personal data, as a form of preventive measure against failures to

protect the personal data the ESP manages. The PDP Regulations do not further elaborate on the forms of this internal documentation.

Law stated - 20 May 2022

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

The PDP Regulations do not recognise the concept of a data protection officer. Therefore, appointing a data protection officer is not mandatory under Indonesian law. However, MOCI Regulation No.20/2016 requires that individuals be informed of the contact details of a designated contact person for enquiries into the data processing activity of an ESP. The PDP Regulations do not specifically regulate sanctions for failure to comply with this requirement. However, this may change shortly with the enactment of the Personal Data Protection Draft Bill.

Law stated - 20 May 2022

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

In general, an ESP is required to implement internal guidelines or policies for the collection, processing, and transfer of personal data and implement an audit record related to the provision of its electronic system. Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) also requires ESPs to record processing activities within their electronic systems, including personal data processing.

Law stated - 20 May 2022

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

While there are no specific rules for risk assessment in relation to certain uses of PI, pursuant to GR 71/2019, ESPs must apply risk management to prevent possible damage or loss, which includes conducting risk analysis and formulating mitigation measures and countermeasures to the threats within the electronic systems they manage, which may also contain PI.

Law stated - 20 May 2022

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

To the best of our knowledge, there is no obligation in relation to how PI processing systems must be designed. However, an ESP will be required to implement certain technical and organisational measures when processing personal data.

Law stated - 20 May 2022

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

To the best of our knowledge, PI owners or processors of PI are required to obtain a certificate of registration as an electronic system provider (ESP). Apart from registration as an ESP, we do not believe that there is presently any other obligation for owners or processors of PI to register with the Minister of Communication and Informatics (MOCI).

Law stated - 20 May 2022

Other transparency duties

Are there any other public transparency duties?

To the best of our knowledge, presently other than the obligation to register as an ESP, there is no other obligation for owners or processors of PI to register with the MOCI.

Law stated - 20 May 2022

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

To the best of our knowledge, there is no specific provision that governs outsourced processing services under the PDP Regulations. The current PDP Regulations do not differentiate between the data controller and data processor.

In this regard, there is a general requirement to obtain a legal ground for outsourcing processing services, as they constitute an act of processing. In practice, an electronic system provider (ESP) may include these outsourced processing activities in the notice or privacy policy (or consent request form, if using consent). Further, should the outsourced services involve transnational data transfers, certain requirements need to be complied with under Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016) by submitting a report of the cross-border transfer of personal data, both before and after conducting the transnational transfer. In practice, this report may be submitted annually to the MOCI.

Law stated - 20 May 2022

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Other than a general requirement requiring consent to collect personally identifiable information, to the best of our knowledge, there are no specific restrictions on the sharing of personal data within Indonesia, except for prohibited

data including but not limited to that related to terrorism, child pornography or content that disturbs public order.

Law stated - 20 May 2022

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The PDP Regulations do not restrict international data transfers, except for by public scope ESPs. However, MOCI Regulation 20/2016 requires that the transfer of data overseas be done in coordination with the MOCI.

Law stated - 20 May 2022

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

In this regard, a general requirement shall apply equally to the transfers to service providers and onward transfers (both by the service providers or PI owners). This shall follow relevant provisions related to PI and the requirement to coordinate with the MOCI as regulated under MOCI Regulation 20/2016.

Law stated - 20 May 2022

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

If PI is contained in an electronic system or as data, then it is subject to the provisions on electronic systems and data protection under Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019). According to GR 71/2019, for public ESPs, PI should be retained in Indonesia. PI may be retained outside Indonesia only if the required technology or equipment is not available domestically. However, private ESPs may retain the PI in Indonesia and outside Indonesia. If the PI is retained outside Indonesia, private ESPs must ensure that the relevant Indonesian ministries and agencies are able to effectively monitor the overseas retention of such PI.

Law stated - 20 May 2022

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

The PDP Regulations provide that individuals as data subjects have the right to access their personal information held by PI owners. Other than the right to access, individuals as data subjects also have the rights as well as the limitation of rights as follows:

- the right of access to data or copies of data;

- the right to the rectification of errors;
- the right to the deletion or the right to be forgotten;
- the right to object to processing;
- the right to restrict processing;
- the right to data portability;
- the right to withdraw consent;
- the right to object to marketing; and
- the right to complain to the relevant data protection authority.

Law stated - 20 May 2022

Other rights

Do individuals have other substantive rights?

Other than the right of individuals to access their personal information, Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) acknowledges the right of delisting, which is the right of data subjects to have their personal data removed from search engines provided that the data is no longer 'relevant', based on a court order. The PDP Regulations do not elaborate on when personal data is considered 'irrelevant'. Nonetheless, we are of the view that the same rationale as to why data subjects may have their data erased if they withdraw consent should apply here.

Law stated - 20 May 2022

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) (MOCI Regulation 20/2016) acknowledges the right of data subjects to complain to the MOCI for the failure of an electronic system provider (ESP) to protect their personal data. Data subjects may submit a written complaint to the Directorate General of Application of Informatics (DGAI) within 30 business days from the discovery of the failure to protect the personal data of the data subject. If a violation is found, the DGAI may recommend that the MOCI impose certain administrative sanctions on the ESP. MOCI Regulation 20/2016 does not specifically mention the criteria for loss, but under the Indonesian Civil Code liability to compensate damages based on tort (an unlawful act) can be enforced if certain criteria are fulfilled – namely, an unlawful act and losses (ie, actual losses, damaged reputations or the PI owner has lost commercial opportunities), and there is a causal relationship between the unlawful act and the losses.

Law stated - 20 May 2022

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The MOCI or the DGAI, as the institution mandated by the MOCI to resolve such disputes, shall resolve the dispute through deliberation to reach a consensus or through any alternative mechanism. The official or institution in charge of

settling such a dispute may provide a recommendation to the MOCI for the imposition of administrative sanctions on the breaching ESP. If the dispute resolution is ultimately unsuccessful the personal data owner and the other relevant ESPs may submit a civil claim against the ESP in breach.

Law stated - 20 May 2022

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

There are no derogations, exclusions, or limitations other than those already described, such as the requirement that the overseas transfer of data be done in coordination with the Minister of Communication and Informatics.

Law stated - 20 May 2022

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The PDP Regulations do not regulate the use of cookies.

Law stated - 20 May 2022

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

The PDP Regulations do not regulate this matter. However, we understand that more stringent rules may apply in specific cases, for example, in the financial services sector. Pursuant to Financial Services Authority (OJK) Regulation No. 1/POJK07/2013 regarding Financial Consumer Protection (6 August 2013), as last amended by OJK Regulation No. 18/POJK07/2018 (10 September 2018), a financial service provider is prohibited from disclosing customer data or information to third parties unless they receive written consent from the customer or are required to by law. If a financial service provider obtains the data or personal information of a person or a group of persons from a third party, it is required to obtain written confirmation from the third party that the person or group of persons has agreed to the disclosure. The above rules commonly apply to unsolicited ads or marketing communications by email, and telemarketing telephone calls or text messages.

We are not aware of any other rules pertaining to the sending of electronic direct marketing materials.

Law stated - 20 May 2022

Targeted advertising

Are there any rules on targeted online advertising?

There are no express rules on targeted online advertising. However, according to the PDP Regulations, unless provided otherwise by the laws and regulations, use of any information through electronic media that involves the personal data of a person must be done with the consent of the person concerned. Any person whose rights are infringed may claim

for damages under this law.

Law stated - 20 May 2022

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

The PDP Regulations do not expressly recognise sensitive categories of personal information. However, for private electronic system providers, Minister of Communications and Informatics Regulation No. 5 of 2020 regarding Private Electronic Systems Providers (24 November 2020), as amended by Law No. 10 of 2021 (21 May 2021) recognises specific categories of PI, which consist of health data and information, biometric data, genetic data, sexual orientation, political views, data of children, personal financial data, and/or other data in accordance with the provisions of laws and regulations.

Law stated - 20 May 2022

Profiling

Are there any rules regarding individual profiling?

The PDP Regulations do not regulate this matter.

Law stated - 20 May 2022

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The PDP Regulations do not regulate this matter.

Law stated - 20 May 2022

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Indonesian House of Representatives (DPR) is in the process of finalising the Personal Data Protection Draft Bill (the PDP Draft Bill), which has been included by the DPR in the National Legislation Programme for 2022. The National Legislation Programme is a compilation of the top 50 draft bills that the DPR aims to ratify during the current five-year term of DPR members. However, despite being included in the National Legislation Program, there is no certainty as to when the PDP Draft Bill will be passed into law.

The current Draft Bill heavily resembles Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) of the European Union. In brief, the PDP Draft Bill is intended to clarify the scope of personal data, the roles and responsibilities of data controllers, data processors and data protection officers, and acknowledges most, if not all, of the rights of data subjects under the GDPR, and the general principles on consent to data processing.

Law stated - 20 May 2022

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	Thompson Dorfman Sweatman LLP
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Legal Consultants
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
Mexico	OLIVARES
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitão, Galvão Teles, Soares da Silva & Associados

Singapore	Drew & Napier LLC
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP