Data Protection & Privacy 2020

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2012
Eighth edition
ISBN 978-1-83862-146-9

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2020

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the eighth edition of *Data Protection and Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Hungary, Iceland, Indonesia and Malaysia.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting The Deal Through

London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

Contents

Indonesia

Abadi Abi Tisnadisastra, Prihandana Suko Prasetyo Adi and Filza Adwani
AKSET Law

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The protection of personal data in Indonesia was initially focused on the protection from privacy perspective. Under the Indonesian Constitution, the concept of privacy rights has been recognised and protected as part of the general concept of human rights.

With the need to cover the sector yet to be regulated, specifically that of the internet and electronic transaction related activities, Law No. 11/2008 on Electronic Information and Transactions as amended by Law No. 19/2016 (collectively, the EIT Law) was passed. Even though most of the provisions of the EIT Law focus on electronic transactions, there is a notable provision that deals with personal data in the EIT Law.

Similar with the individual concept in the Indonesian Constitution, article 26(1) of the EIT Law (along with its official elucidation) recognises the protection of personal data as a part of privacy rights. The article further mentions that privacy rights shall include, among others, the right to monitor the access of information concerning private life and data. To further the effort to satisfy the need for effective protection of personal data, the Minister of Communications and Informatics (the MoCI) issued MoCI Regulation No. 20/2016 on Protection of Personal Data in Electronic Systems (MoCI Regulation 20).

MoCI Regulation 20 is issued as mandated under article 15(3) of Government Regulation No. 82/2012 on the Implementation of Electronic Systems and Transactions (GR 82), which requires personal data protection in electronic systems to be regulated by a Ministerial Regulation. MoCI Regulation 20 came into effect on 1 December 2018, and it applies only to PII stored in electronic systems, but not to PII that is stored manually.

It is important to note that in comparison to other jurisdictions, which commonly formed their data protection regulations based on international instruments (eg, the EU General Data Protection Regulation (GDPR)), the current data protection law regime in Indonesia is still less developed. MoCI Regulation 20 does not recognise a number of concepts, such as, data controller, data processor, sensitive personal data, dedicated data protection officer, privacy by design, and automatic processing. Nevertheless, certain general principles in GDPR related to the processing of personal information have been adopted by MoCI Regulation 20, among others, lawfulness, confidentiality, the purpose of limitation, accuracy and storage limitation.

Other than the above legislation, the protection of personal data is also included in several laws and regulations, though most of these laws and regulations only address data protection briefly:

- Law No. 7/1992 regarding Banking as amended by Law No. 10/1998 (the Banking Law);
- Law No. 39/1999 regarding Human Rights;
- Law No. 23/2006 regarding Resident Administration as amended by Law No. 24/2013 (the Resident Law);
- Law No. 36/1999 regarding Telecommunications (Telecommunications Law);
- Law No. 14/2008 regarding Transparency of Public Information;
- Law No. 36/2009 regarding Health (the Health Law);
- Minister of Health Regulation No. 269/Menkes/Per/III.2008 on Medical Records (MoH Regulation 269);
- MoCI Regulation No. 36 of 2014 on the Registration Procedure of Electronic System Operator; and
- MoCI Regulation No. 4 of 2016 on the Information Security Management System (MoCI Regulation 4).

Given the need to have a dedicated data protection law in force, at the moment, the Indonesian government and House of Representative have included a personal data protection bill (the PII Bill) in the national legislative programme.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no specifically dedicated national data protection authority that oversees personal data protection in Indonesia. However, pursuant to MoCI Regulation 20, the MoCI (along with the Director General of Informatics Applications or Ditjen Aptika) are responsible for ensuring compliance towards the data protection regime in Indonesia (ie, EIT Law, GR 82 and MoCI Regulation 20).

The MoCI is authorised to, among others, organise governmental events related to communications and informatics; coordinate with Electronic System Operators (ESOs) for transfer of personal data overseas; settle disputes related to failure or breach of PII protection; supervise the implementation of personal data protection; request data and information from ESOs in the framework of data protection; impose administrative sanctions for violations data protection regulations; and issue Electronic System Worthiness Certificate to certify that an electronic system is functioning properly.

For certain specific matters, such as, in the event of a dispute related to the failure or breach of personal data protection, MoCI may delegate its authority to Ditjen Aptika that is authorised to form a panel to settle the disputes and recommend certain administrative sanctions to be imposed by the MoCI on relevant ESOs. Ditjen Aptika is also responsible for conducting public education on matters related to personal data protection.

In addition, for a specific sector (ie, financial sector), each sectoral supervision and regulation body has the authority to regulate the relevant matters related to the data protection as well.

Cooperation with other data protection authorities

3 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??

Under MoCI Regulation 20, the MoCI may coordinate with the sectoral supervision and regulatory body to follow up on complaints lodged by data subjects for failures of personal data protection committed by ESOs.

These two authorities may also cooperate to supervise the implementation of MoCI Regulation 20, including to impose administrative sanctions for breaches of MoCI Regulation 20. Under MoCI Regulation 20, the MoCI delegates the authority to settle PII disputes to Ditjen Aptika, which may then form a panel to settle the disputes. The MoCI also delegates the supervision of the implementation of MoCI Regulation 20 to Ditjen Aptika.

Particularly for cooperation with foreign authorities in certain specific matters, such as transnational data transfer, at the moment, we are not aware of the existence of any cooperation entered into by the MoCI with foreign authorities, nor has the Indonesian government published a list of persuasive countries considered to have an adequate level of protection with respect to transnational data transfer.

Breaches of data protection

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

Breach of data protection might be subject to administrative and criminal liability in Indonesia. As a rule of thumb, under MoCI Regulation 20, any person that collects, processes, analyses, stores, promotes, announces, transmits or publishes personal data without the right to do so will be subject to certain administrative sanctions, such as verbal warning; written warning; suspension of activities; or announcement on the relevant website.

In addition, failure to comply with GR 82 will also be subject to similar administrative sanctions, comprising of written warning; administrative fines; temporary dismissal; or dismissal from the list of registrations.

Under the EIT Law, breach of privacy is also subject to criminal penalties, as follows:

- a fine of 600 million up to 800 million Indonesian rupiah and six to eight years' imprisonment for unlawful access;
- a fine of 2 billion up to 5 billion Indonesian rupiah and eight to 10 years' imprisonment for alteration, addition, reduction; transmission, tampering, deletion, moving or hiding electronic information or electronic records; and
- a fine of 800 million Indonesian rupiah and 10 years' imprisonment for interception or wiretapping of a transmission.

In addition, under the Telecommunication Law, any person is prohibited from wiretapping information transmitted through telecommunication networks. A person violating this prohibition may be sentenced to imprisonment of up to 15 years.

Under the Resident Law, failure to protect personal data may be subject to imprisonment for up to two years or a fine of up to 25 million Indonesian rupiah, or both. The Resident Law classifies the following information as protected personal data: information regarding physical and mental disabilities, fingerprints, irises, signatures, and other data that relate to a person's crime.

A criminal proceeding is initiated by the Indonesian police and prosecutors.

SCOPE

Exempt sectors and institutions

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

In essence, the EIT Law, GR 82 and MoCI Regulation 20 are only applicable to all processing or use of personal data in electronic form by an ESO, which is defined as any person, state administrator, business entity, and community that provides, manages or operates an electronic system, whether individually or jointly, for the electronic system's users' own interests or the interests of other parties.

For the purpose of this definition, electronic systems are defined broadly as series of devices and electronic procedures used to prepare, collect, process, analyse, store, display, announce, deliver or disseminate electronic information.

Based on the foregoing, at the moment, although processing or use of personal data in a manual record is excluded from the scope of the above regulations, but when it comes to the protection of personal data in the electronic system, ESOs have the responsibility to comply with the relevant regulations, regardless of the sectors and type of organisations.

As a fundamental principle, Indonesia adopts a consent regime to obtain and process personal data through the electronic system. Prior consent of the data subject is not required if obtaining or collecting personal data is mandated by law or certain personal data has been transmitted or announced publicly by electronic systems for public services.

Certain exemptions are also applicable in the banking sector. In principle, banks are required to maintain confidentiality of information concerning savings of customers except for special circumstances – namely, taxation purposes, settlement claims and interbank exchange of information.

Communications, marketing and surveillance laws

6 Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The right to privacy is considered as a basic human right. The interception of communications is governed by the EIT Law and the Telecommunications Law, which stipulate that any illegal interception or wiretapping shall be subject to certain criminal sanction (see question 4). However, exemptions apply for lawful interception or wiretapping in the framework of law enforcement, such as in a corruption case investigation.

Other laws

7 Identify any further laws or regulations that provide specific data protection rules for related areas.

There are no specific regulations regarding the monitoring of employees specifically through electronic systems. In this regard, so long as the information of such employee falls under the definition of personal data (see question 7), any monitoring activities shall obtain consent from the employees.

For healthcare data, the processing shall comply with Health Law No. 36 of 2009 and MOH Regulation 269. Under article 57 of the Health Law, every person is entitled to the confidentiality of his or her private

health conditions that have been disclosed to healthcare providers. These private health conditions, which under MOH Regulation 269 are defined as medical records, shall be considered as personal data.

While for the use of social media, although the information posted on a user's public profile could be considered as public information, the collection and the processing of user content are still subject to data protection regulations (ie, the obtainment of consent from the user).

Particularly for data protection in the bank sector, customer's private data (ie, credit information) are considered confidential bank information. Any disclosure of such information shall be based on prior written consent from the customer.

PII formats

8 | What forms of PII are covered by the law?

The current definition of personal data under MoCI Regulation 20 is very broad and is likely to include most of the information that is related to an individual or can be used to identify a certain individual. As for the format, the applicability of the MoCI Regulation 20 applies only to personal data stored in electronic systems, and not applicable for personal data that is stored manually.

In addition, although the current personal data regulation only applies to inherent and identifiable information (either directly or indirectly), there is no specific requirement for the data to be anonymised before disclosure or transfer to the third party. However, any personal data to be processed must be encrypted.

The current regulations do not elaborate on the types of personal data.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The EIT Law, as an umbrella regulation on data protection in Indonesia, has extraterritorial coverage and it applies to a foreign legal subject (with or without a legal presence) having legal effect in Indonesia. However, at the moment, the enforcement of the EIT Law and its implementing regulations against a foreign entity on data protection related matters is relatively remote.

Covered uses of PII

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

There is no specific definition of 'processing' under MoCI Regulation 20. However, for processing purpose, MoCI Regulation 20 actually adopts reference to certain operations on personal data within the electronic system that can be regarded as processing of personal data, namely, collection, analyses, processing, storage, display, announcement, transmission, disclosure, access or disposal of personal data or information.

With respect to the parties involved in the processing, unlike in some other jurisdictions, there is no distinction is made between those who control personal data and those who provide services to process personal data on behalf of the controller. Therefore, ESOs have the responsibility to comply with data protection regulations.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

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

The regulations do not provide any specific grounds for personal data processing other than consent. In brief, under MoCI Regulation 20, processing activities must be based on prior consent from the data subject and the data in question have been verified, and the action is in accordance with the purpose for which the personal data was collected or otherwise processed. In addition, MoCI Regulation 20 does not offer common legal bases for the processing of personal data, such as the processing of data being necessary for the vital interest or the processing activities are carried out based on legitimate interest.

Particularly for the consent, opposed to a common regulatory approach, the Indonesian regulatory framework does not specifically elaborate on the requirement of valid consent – namely, whether consent should be freely given, and separate consent shall be prepared.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

There is no distinction between the types of personal data in the regulations. All information is regarded as personal data and has the same protection treatment. Indonesia does not adopt the concept of sensitive personal data either.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

MoCI Regulation 20 require an ESO to notify the data subjects for the processing of personal data, through which the ESO also obtains the user's consent. Other than the requirement that the consent needs to be in writing (either manually or electronically) and be prepared in Bahasa Indonesia, MoCI Regulation 20 does not expressly regulate the content of the consent. In practice, the notification usually covers the collected information, processing purposes and activities, the possibility to share or transfer collected information, access towards collected information, contact details of the ESO and so on.

Exemption from notification

14 | When is notice not required?

See question 5.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

There are no express provisions in the PII protection regulations that compel ESOs to offer data subjects a degree of choice of control over the use of their PII. However, MoCI Regulation 20 regulates that data subjects are entitled to the confidentiality of their PII. Data subjects may inform the ESO which of their PII must be kept confidential or

non-confidential. The data subjects are also allowed to revoke their consent and to request that their PII be deleted.

Data accuracy

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

MoCI Regulation 20 provides that PII collection and processing must be confined only to relevant information in accordance with the purpose of the collection of the PII and must be done accurately. Management, analysis and storage of PII by an ESO must be done only after the PII has verified its accuracy. The ESO is obligated to maintain the accuracy of PII from collection until its deletion. Further, data subjects are entitled to renew or amend their PII stored without distressing the PII management system.

Amount and duration of data holding

17 Does the law restrict the amount of PII that may be held or the length of time it may be held?

Data subjects are entitled to request the ESO delete their PII, and the ESO must do so accordingly. If the data subject does not request such deletion, under MoCI Regulation 20, an ESO shall comply with a five-year minimum statutory retention period or as otherwise required by the relevant supervisory authority. This retention period is calculated from the moment the data subject terminates the use of services of the ESO.

Following the expiration of the retention period, the ESO may delete the relevant personal data, unless the ESO determines that the personal data is still required to be kept and used in accordance with the purpose for which it has been processed. For the latter, the ESO shall obtain consent from the data subject and shall provide sufficient information on why the ESO retains the relevant personal data (ie, the information on the category of personal data and the purpose of the processing).

Finality principle

18 Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes, the PII shall serve the purpose for which it was collected, as notified to the data subject. An ESO shall also ensure that the processing of PII shall be in line with the specific purpose that has been consented to the data subject.

Use for new purposes

19 If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

MoCI Regulation 20 does not recognise the concept of finality principle. There is no guidance on whether separate consent shall be prepared and obtained for multiple or new purposes of processing personal data. Ideally, to ensure legitimate processing, a separate new notice and consent would be required if the ESO intends to collect, use, disclose or transfer the PII for new purposes other than those for which the data subject had given consent.

SECURITY

Security obligations

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

Under GR 82 and MoCI Regulation 20, an ESO has a general obligation to maintain confidentiality, implement adequate security and organisational measure, and develop internal data protection policy. In addition, for the purpose of security measure for PII protection, MoCI Regulation 20 requires the following:

- an electronic system that is used for obtaining and collecting PII must have the capacity of interoperability and compatibility;
- electronic systems must use legal software;
- electronic systems used in the process must be certified;
- PII which is stored in an electronic system must be in the form of encrypted data;
- storage of PII in an electronic system must be performed in accordance with the provisions regarding the procedures and facilities for securing the electronic system;
- an ESO shall use (establish or rent) a data centre and disaster recovery centre located within the territory of Indonesia (for an electronic system for public purposes) and fulfil the minimum standards in information technology systems, information technology risk management, information technology safeguards, resistance to system faults and failure, and transfer of information technology system management;
- an ESO is required to notify the data subject if the ESO's security system has been breached; and
- for overseas transfer of PII, in addition to the general conditions to obtain consent, MoCI Regulation 20 requires a party to (i) coordinate with the MOCI or authorised institutions; and (ii) implement relevant regulations regarding offshore transfer of PII.

In addition, according to MoCI Regulation 4, there is a mandatory certification for an electronic system having a high-level and strategic function (ie, related to sectoral or regional interest, public interest, national defence and security).

Notification of data breach

21 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?

With respect to data breach situation, there is no specific guidance on the scope of a data breach (eg, accidental or unauthorised access, loss of personal data, etc).

As a general reference with respect to security incidents in an electronic system, article 20(3) of GR 82 specifically requires an ESO to notify law enforcement authorities or the relevant sectoral supervisory and regulatory agency (eg, banking or other financial service sector in the event of failure or disturbance of an electronic system caused by outsiders, which results in a serious risk to the electronic system (eg, the system not functioning properly). Therefore, not every security incident requires notification to the authority.

In addition, a strict interpretation of a relevant provision in GR 82 implies that the obligation to notify would be limited to a security incident that involves a third party – that is, attack from outsider to the server(s), which may, among other matters, relate to personal data breaches. However, in practice, breach of personal data does not necessarily result from a security incident (ie, attack by an outsider), but could also be the result of inadequate internal measures (eg, an accidental disclosure

of personal data due to negligence of the internal staff responsible to maintain the confidentiality and protection of personal data).

Separate from the requirement under GR 82 on the notification obligation for security incidents caused by an outsider, GR 82 requires an ESO to notify a data subject (individual) in writing, in the event of a personal data breach within its electronic system. GR 82 does not require an ESO to notify law enforcement authorities or the relevant sector supervisory or regulatory agency about a data breach.

MoCI Regulation 20 requires that relevant written notification to the data subject shall be made within 14 days of the ESO becoming aware of a data breach, and the ESO shall ensure that the data subject receives the notification if the data breach may potentially cause losses to the data subject. However, there are no specific criteria for an occurrence to be considered as a 'loss' under MoCI Regulation 20.

Like GR 82, there is no specific provision in MoCI Regulation 20 that requires an ESO to also provide notification about security incidents associated with a personal data breach situation to law enforcement authorities or the relevant sectoral supervisory or regulatory agency at the same time as the notification to the affected data subject.

MoCI Regulation 20 further stipulates that the notification may be delivered electronically to the data subject, provided that consent has been given for such method by the data subject concerned. In light of specific communication channel to notify the data subject, since MoCI Regulation 20 is silent on this matter, it is advisable for the ESO to implement several communication channels (ie, email, direct message, etc) directly to the affected data subject for the purpose of ensuring that the message is properly received by the relevant individual.

For data breach notification, MoCI Regulation 20 only provides minimum mandatory information that needs to be included in the notification. In this regard, article 28 (c)(1) of MoCI Regulation 20 only specifically requires information on the reasons for the data breach to be included in the notification to the data subject. Meanwhile, other relevant information such as:

- the types of personal data and approximate numbers of the affected data subject;
- the impact of data breach; and
- any security measures that the ESO has implemented or will implement to handle the data breach situation is not specifically requested to be mentioned in the notification. Since the foregoing information is normally mentioned in the data breach notification, if possible, it is advisable for an ESO to include that relevant information in its standard data breach notification.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

There is no requirement for an ESO to have a dedicated data protection officer in Indonesia. However, MoCI Regulation 20 requires an ESO to provide a contact person who is accessible to respond to any communication request from a data subject.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

As part of its effort to maintain the security of its electronic system, an ESO is required to implement internal guidelines or policy for the collection, processing, and transfer of personal data and implement an audit record related to the provision of its electronic system.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

There are no obligations in the relevant regulations for an ESO to implement data protection by design and by default or to implement a privacy impact assessment. However, MoCI Regulation 20 does require an ESO to implement certain technical and organisational measures when processing personal data.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

Other than the obligation to obtain a registration certificate as an electronic system operator for an ESO for public purposes, there is presently no obligation under the prevailing regulations for an ESO that collects and processes personal data to be registered with the MoCI.

Formalities

26 | What are the formalities for registration?

See question 25.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

See question 25.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

See question 25.

Public access

29 | Is the register publicly available? How can it be accessed?

See question 25.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

See question 25.

Other transparency duties

31 | Are there any other public transparency duties?

There is presently no requirement for an ESO to make public statements related to its processing activities.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

There is no specific provision under MoCI Regulation 20 that governs outsourced processing services. In this context, a general requirement to obtain consent shall also be applicable to this outsourcing service.

Should the outsourcing services involve transnational data transfer, certain requirements need to be complied with (see questions 34 and 35).

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

Other than a general requirement to obtain consent and to comply with relevant provisions related to PII protection (ie, based on prior consent, the collected data must have been verified, and the action must comply with the purpose of limitation principle), there are no specific restrictions on the transfer of personal data within Indonesia.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

Other than the general requirement of permissible data transfer as mentioned in question 33 and the compliance of coordination requirement (see question 35), the transfer of PII outside Indonesia does not require an ESO to implement specific regulations regarding offshore transfer of personal data.

At the time of writing, there is no restriction on transferring personal data to any country abroad nor a requirement that personal data shall be adequately protected when being transferred outside Indonesia. Neither has the Indonesian government entered into any arrangement with another country to set any 'safe harbor' scheme or similar arrangement related to the transfer of personal data outside Indonesia.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Cross-border transfer of PII does not require prior authorisation, but it does trigger a requirement to coordinate with MoCI as required under MoCI Regulation 20, by way of submitting a report of an overseas transfer of personal information both before and after conducting the transfer. Such report shall include at least information on the designated country, recipient, date of transfer, and reason or purpose of the transfer. If necessary, an ESO may also request advocacy assistance from the MoCI, particularly for obtaining clarity on transnational personal data flows before submitting the relevant report to the MoCI.

Further transfer

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

Requirements similar to those mentioned in question 34 are applicable to the onward transfer of PII to service providers.

RIGHTS OF INDIVIDUALS

Access

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

MoCI Regulation 20 stipulates that the PII owner shall have the rights to access his or her personal data, which allows the PII owner to change, add and update his or her personal data. Additionally, the regulation opens an opportunity for deletion of data based on the request of PII owner who has intentionally revoked the consent. PII owner is also entitled to obtain the history of their personal data that was shared to third parties.

Other rights

38 | Do individuals have other substantive rights?

See question 37.

Compensation

39 | 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?

MoCI Regulation 20 provides the right to claim for damages if an ESO fails to comply with the consent regime. In addition, in the event of a data breach, a data subject may also file a claim to Ditjen Aptika if an ESO fails to notify the data subject in writing about a data breach (see question 21) or if there is a loss resulting from a data breach situation.

For the latter, although MoCI Regulation 20 does not specifically mention the criteria of loss, under the Indonesian Civil Code, liability to compensate damages based on tort (unlawful act) can be enforced if certain criteria are fulfilled – namely, an unlawful act, losses (ie, actual loss, reputations have been damaged or that the PII owner has lost commercial opportunities), and causal relationship between the unlawful act and the losses.

Enforcement

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

For the claim to be submitted to Ditjen Aptika, the intention is to resolve the claim amicably or by way of alternative dispute resolutions. In any case, the PII owner has the rights to seek the recovery of monetary damages or compensation through the judicial system in a civil proceeding.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

There is no additional derogation, exclusions or limitation other than those already described (see question 5).

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Although no specific provision in MoCI Regulation 20 mentions the possibility for a PII owner appeal against an order of the supervisory authority, there is no restriction for a PII owner to take necessary action (ie, appeal to a court) if the PII owner is not satisfied with the order.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

Specific rules on the use of 'cookies' are not mentioned in any regulations related to data protection in Indonesia. However, the current broad interpretation of personal data may likely include 'cookies' as personal data. Hence, while there might be no expectation for an ESO or the data subject that the information on the cookies should be treated as private information, the use of such technology may require compliance with MoCI Regulation 20.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

There are presently no specific rules on marketing by email in Indonesia. However, as the ITE Law acknowledges, the concept of privacy, at the minimum, the general requirement to conduct marketing based on consent would apply. On the other hand, there is a prohibition for a telecommunications content provider or network operator to offer or facilitate the offer of certain content to consumers if the consumers do not agree to receive the content.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

Given the broad definition of electronic system that includes cloud infrastructure, the processing of personal data within cloud-based infrastructure shall also be subject to the requirements to provide adequate security measures and prevent any possible data breach.

In addition, although the current legislation does not provide any guidance on the use of cloud-based technology with respect to the processing of personal data, as a general rule, storing personal data in the cloud may also constitute a transfer of personal data (either national or transnational transfer) depending on the location of the cloud's server. An ESO for the public purpose must maintain a data centre and data recovery centre within Indonesia.

For data sharing or data transfer arrangements with a cloud-based provider, there is no specific obligation under the Indonesian regulatory framework for the data collector to have a contract for the processing of personal data by way of a processor. In essence, when a data collector and a cloud-based provider have an arrangement to process personal data, the cloud-based provider would be regarded merely as an ESO rather than a data processor acting under the instruction of a data collector. In this case, both companies bear the responsibility to be an ESO and will be required to meet their obligations under the EIT Law, GR 82 and MoCI Regulation 20.

UPDATE AND TRENDS

Key developments of the past year

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

In addition to the discussion of the PII Bill, the MoCI is in the process of amending several provisions in GR 82, including relevant provisions related to data localisation.

In brief, the proposed revision on the assessment of data localisation requirement will not automatically require ESOs to establish a data centre or disaster recovery centre. However, it will depend on the type of data. Based on the current draft, there will be three possible data classifications – namely, strategic data, high-risk data and low-risk data. Low-risk data that is not regarded as strategic data or high-risk data may be stored offshore so long as it can be accessed in Indonesia (sectoral regulation may determine otherwise).

Note that the PII Bill and draft government regulation to amend GR 82 are still being finalised and the substance of the PII Bill and the proposed amendment of GR 82 remains to be seen.

Abadi Abi Tisnadisastra
atisnadisastra@aksetlaw.com

Prihandana Suko Prasetyo Adi
pprasetyoadi@aksetlaw.com

Filza Adwani
fadwani@aksetlaw.com

29th Floor, The Plaza Office Tower
Jl M H Thamrin Kav 28-30
Jakarta – 10350
Indonesia
Tel: +62 21 2992 1515
www.aksetlaw.com

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN 978-1-83862-146-9