Data Protection & Privacy 2022

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 manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Tenth edition
ISBN 978-1-83862-644-0

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

Data Protection & Privacy

2022

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

Lexology Getting The Deal Through is delighted to publish the tenth edition of *Data Protection & 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 Jordan, Pakistan and Thailand.

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 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction 5
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

EU overview 11
Aaron P Simpson, David Dumont, James Henderson and Anna Pateraki
Hunton Andrews Kurth LLP

The Privacy Shield 14
Aaron P Simpson and Maeve Olney
Hunton Andrews Kurth LLP

Australia 20
Alex Hutchens, Jeremy Perier and Meena Muthuraman
McCullough Robertson

Austria 28
Rainer Knyrim
Knyrim Trieb Rechtsanwälte

Belgium 37
David Dumont and Laura Léonard
Hunton Andrews Kurth LLP

Brazil 49
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra
Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados

Canada 57
Doug Tait and Kendall N Dyck
Thompson Dorfman Sweatman LLP

Chile 65
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
Magliona Abogados

China 72
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

France 82
Benjamin May and Marianne Long
Aramis Law Firm

Germany 96
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

Hong Kong 104
Gabriela Kennedy, Karen H F Lee and Cheng Hau Yeo
Mayer Brown

Hungary 113
Endre Várady and Eszter Kata Tamás
VJT & Partners Law Firm

India 121
Arjun Sinha, Mriganki Nagpal and Siddhartha Tandon
AP & Partners

Indonesia 128
Rusmaini Lenggogeni and Charvia Tjhai
SSEK Legal Consultants

Israel 136
Adi El Rom and Hilla Shribman
Amit Pollak Matalon & Co

Italy 145
Paolo Balboni, Luca Bolognini, Davide Baldini and Antonio Landi
ICT Legal Consulting

Japan 154
Akemi Suzuki and Takeshi Hayakawa
Nagashima Ohno & Tsunematsu

Jordan 164
Ma'in Nsair, Haya Al-Erqsousi and Mariana Abu-Dayah
Nsair & Partners - Lawyers

Malaysia 170
Jillian Chia Yan Ping and Natalie Lim
SKRINE

Malta 178
Paul Gonzi and Sarah Cannataci
Fenech & Fenech Advocates

Mexico 187
Abraham Díaz and Gustavo A Alcocer
OLIVARES

New Zealand 195
Derek Roth-Biester, Megan Pearce and Victoria Wilson
Anderson Lloyd

Pakistan 202
Saifullah Khan and Saeed Hasan Khan
S.U.Khan Associates Corporate & Legal Consultants

Portugal 209
Helena Tapp Barroso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Romania 218
Daniel Alexie, Cristina Crețu, Flavia Ștefura and Alina Popescu
MPR Partners

Russia 226
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva and Alena Neskoromyuk
Morgan, Lewis & Bockius LLP

Serbia 235
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 242
Lim Chong Kin
Drew & Napier LLC

Sweden 257
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 265
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Taiwan 276
Yulan Kuo, Jane Wang, Brian Hsiang-Yang Hsieh and Ruby Ming-Chuang Wang
Formosa Transnational Attorneys at Law

Thailand 284
John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Patchamon Purikasem
Formichella & Sritawat Attorneys at Law Co, Ltd

Turkey 291
Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen and Nazlı Bahar Bilhan
Turunç

United Kingdom 299
Aaron P Simpson, James Henderson and Jonathan Wright
Hunton Andrews Kurth LLP

United States 309
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Indonesia

Rusmaini Lenggogeni and Charvia Tjhai

SSEK Legal Consultants

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?

Indonesia has yet to enact a data protection regulation that would apply to PII. Currently, the closest regulatory regime that exists in Indonesia is the protection of PII within one specific enumerated context. The provisions on the protection of PII 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); 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).

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 the end of 2021, but the covid-19 pandemic could delay that.

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) 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.

Data protection authority

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

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.

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.

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?

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.

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?

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-mentioned 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 rupiahs to 800 million rupiahs or four to eight years' imprisonment for unlawful access;
- fines of 800 million rupiahs to 1 billion rupiahs or six to 10 years' imprisonment for interception or wiretapping of a transmission;
- fines of 2 billion rupiahs to 5 billion rupiahs 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 rupiahs to 12 billion rupiahs 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.

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?

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 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: Government Regulation No. 71 of 2019 regarding the Provision of Electronic Systems and Transactions (4 October 2019) (GR 71/2019) 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.

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.

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 rupiahs 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.

Other laws

7 Identify 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.

PII formats

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

The definition of personal data has evolved throughout the enactment of the PDP Regulations. Minister of Communication and Informatics 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.

Extraterritoriality

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

Article 2 of the Electronic Information Law provides that it has an extra-territorial 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.

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?

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 'data controllers' primarily refer to ESPs.

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 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 other 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.

Legitimate processing – types of PII

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

Indonesia does not recognise a distinction between the types of personal data. Indonesia recognises that all information is personal data and shall receive the same protection.

However, we understand that more stringent rules may apply in specific cases, for example in the financial services sector. Under OJK Circular Letter No. 14/SEOJK07/2014 on Confidentiality and Security of Consumers Personal Data or Information, 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 consent or as is obligated by laws and regulations.

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?

The PDP Regulations recognise the term transparency. For example, Electronic System Providers (ESPs) must notify data subjects of data breaches within 14 days after the discovery of such 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 Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) do provide more clarity on how the required consent is to be given.

MOCI Regulation 20/2016 defines 'consent' as:

> *a written manual or electronic statement given by a personal data owner after receiving complete disclosure of the acquisition, collection, processing, analysis, storage, display, announcement,*

transfer and disclosure, as well as the confidentiality or non-confidentiality, of the personal data.

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.

Exemption from notification

14 | 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.

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?

Generally, article 26(1) of the Electronic Information Law provides that any actions taken concerning personal data must be based on the consent of the data subject. ESPs will require consent to be both broad and as specific as possible, covering, among other things, transfer of the collected data to the 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. To the best of our knowledge, there are no express provisions in the PDP Regulations that compel ESPs to offer data subjects a degree of choice of control over the use of their data.

Data accuracy

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

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 PII from collection to its deletion.

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 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.

Finality principle

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

Yes, 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.

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?

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 be following the original purpose of its processing.

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

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII 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. To date, no such regulation has been issued.

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?

Generally, 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 unofficial confirmation with officials from the MOCI, the MOCI expects to be notified of any data breach.

In this regard, in the event of data breaches, ESPs must notify data subjects within 14 days after the discovery of such breach. In such regard, by nature, an ESP, acting as the controller of data, shall 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 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.

INTERNAL CONTROLS

Data protection officer

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

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, Minister of Communication and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) does require that individuals be informed of the contact details of a designated contact person for enquiries into an Electronic System Provider's (ESP's) data processing activities. 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.

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.

Furthermore, Government Regulation No. 71/2019 on the Operation of Electronic System and Transaction (GR 71) also requires the ESO to record processing activities within their electronic system, including personal data processing.

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?

To the best of our knowledge, PII owners or processors of PII 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 PII to register with the Minister of Communication and Informatics (MOCI).

Formalities

26 | What are the formalities for registration?

Not applicable.

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?

Not applicable.

Refusal of registration

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

Not applicable.

Public access

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

Not applicable.

Effect of registration

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

Not applicable.

Other transparency duties

31 | 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 PII to register with the MOCI.

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?

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.

Restrictions on disclosure

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

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 transfer of personal data within Indonesia.

Cross-border transfer

34 | Is the transfer of PII 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.

Notification of cross-border transfer

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

The cross-border transfer of PII does not require prior authorisation from a government institution, but MOCI Regulation 20/2016 does require coordination with the MOCI by way of submitting a report of an overseas transfer of personal information both before and after conducting the transfer.

There are specific requirements under MOCI Regulation 20/2016 that would enable a company, if considered an ESP, to transfer personal data from Indonesia to abroad. Under article 22(1) of MOCI Regulation 20/2016, an ESP in the private sector may transfer personal data abroad after fulfilling the following requirements:

1 coordinate with the MOCI or officials or agencies authorised to do so; and
2 apply the provisions of laws and regulations regarding the cross-border exchange of personal data.

Article 22(2) of MOCI Regulation 20/2016 further clarifies that such coordination, as referred to in point (1) above, is implemented in the form of:

- reporting the planned transfer of personal data to the MOCI, which includes at least the name of the receiving state and the receiver, frequency of transfer, and the reason or purpose of such transfer;
- requesting advocacy, if necessary; and
- reporting the result of the transfer.

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?

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

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.

The PDP Regulations provide that individuals as data subjects have the right to access their personal information held by PII 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.

Other rights

38 | 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.

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?

Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 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 20/201 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 PII owner has lost commercial opportunities), and there is a 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?

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.

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 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.

SUPERVISION

Judicial review

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

To the best of our knowledge, there is no restriction for a PII owner to take necessary action, such as appealing to a court against any supervisory authority 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.

The PDP Regulations do not regulate the use of cookies.

Electronic communications marketing

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

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) 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 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.

Cloud services

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

The PDP Regulations do not regulate this matter.

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?

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 Program for 2021. The National Legislation Program 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.

SSEK
Indonesian Legal Consultants

Rusmaini Lenggogeni
rusmainilenggogeni@ssek.com

Charvia Tjhai
charviatjhai@ssek.com

14th Floor, Mayapada Tower I
Jl Jend Sudirman Kav 28
Jakarta 12920
Indonesia
Tel: +62 21 521 2038/ +62 21 2953 2000
Fax: +62 21 521 2039
www.ssek.com

Coronavirus

47 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Other than the notification on the issuance of the PDP Draft Bill, we are not aware of any emergency legislation, relief programmes and other initiatives specific to data protection implemented to address the covid-19 pandemic. The current PDP Regulations are still the regulations that regulate personally identifiable information.

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
Business & Human Rights
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
Drone Regulation
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
Healthcare M&A
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
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
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

an LBR business

ISBN 978-1-83862-644-0