CLIENT UPDATE
29 DECEMBER 2016

Personal Data Protection Regime Gets Boost with New Regulation

After a wait of more than a year, the Minister of Communications and Information (the "**Minister**") issued Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems ("**PDP Regulation**") on 1 December 2016. The PDP Regulation, which puts into effect Article 15(3) of Government Regulation No. 82 of 2012 on Electronic Systems and Transactions ("**Electronic Systems and Transactions Regulation**"), sets out the rules governing the protection of personal data that are stored in electronic form. While its scope does not extend beyond electronic data, we nevertheless believe that it should have a sufficiently wide-ranging impact as to significantly strengthen personal data protection in Indonesia, given the vast extent of electronic communications and transactions nowadays.

Personal Data

Prior to discussing the scope of the PDP Regulation, it is important to first understand the definitions of "personal data" and "electronic system provider."

Personal Data Defined

Under the Electronic Systems and Transactions Regulation, and now under the PDP Regulation, "personal data" is defined as:

> "*Certain data related to an individual, of which the (a) accuracy and (b) confidentiality is (i) kept, (ii) maintained and (iii) protected*".

This definition has been adopted word for word from Law No. 23 of 2006 on Population Administration, as amended by Law No. 24 of 2013 ("**Population Administration Law**"), the first legislation in Indonesia to define personal data.

The PDP Regulation also provides a definition of "certain data related to an individual," namely:

> "*All information that is correct and real, and personally identifiable, whether directly or indirectly, with an individual in accordance with the provisions of the laws and regulations in effect.*"

We believe that this definition of "certain data related to an individual" precisely captures the meaning of personal data, i.e., information that can be used to identify a specific person.

Subject of the PDP Regulation

The primary subject of the PDP Regulation is "electronic system providers." An electronic system provider is defined as:

> "*Any person, State authority, business entity or community that provides, manages, and/or operates an electronic system, whether independently or jointly, in the interest of the electronic system's users and/or the interests of other parties*."

This definition includes State authorities. If we go by the letter of the regulation, similar standards will be imposed on the management of personal data by both the public and private sectors. Certain Government ministries and agencies, such as the Financial Supervisory Authority (OJK), the Tax Office and the Ministry of Home Affairs, handle huge amounts of personal data, not to mention state companies

that provide public services, such as the state-owned power utility (PLN) and state-owned telecommunications company (Telkom).

Another aspect of the definition is its broad coverage. A public or private entity is subject to the PDP Regulation not only when it "provides" its own services, but also when it "manages" or "operates" an electronic system, presumably on behalf of a third party. As companies embark on outsourcing or managed-service arrangements, it will be crucial that the compliance obligation is assigned to the right party.

Prior Consent

The PDP Regulation requires any action taken in relation to personal data to have secured the prior consent of the person who is the owner of such personal data. Such actions include (i) acquisition, (ii) processing and analysis, (iii) storage, (iv) dissemination, disclosure and access, and (v) erasure of personal data, or its destruction in the case of a hard-copy record.

In order to secure such consent, the electronic system provider must provide a standard form in Bahasa Indonesia to be agreed by the person who is being asked to provide his/her personal data (the "**Privacy Notice and Consent**"). Note that although a Privacy Notice and Consent must be in Bahasa Indonesia, the PDP Regulation does not preclude the making of versions in other languages.

A Privacy Notice and Consent will primarily set out:

1. The purpose for which the personal data is being requested;
2. How the personal data will be processed; and
3. Rights of the personal data owner, including the right to have their personal data modified or updated, to access their personal data, and to have their personal data deleted or destroyed (in the case of a hard-copy record).

Most importantly, the Privacy Notice and Consent will set out the prior consent of the personal data owner for the actions of the electronic system provider, which, according to the PDP Regulation, may include the acquisition, collection, processing, analysing, storage, display, announcement, transfer, transmission, providing access, and disposal of his/her personal data.

If the personal data owner is a minor, the Privacy Notice and Consent must be agreed to by his or her parents or guardian. Under the Indonesian Civil Code, any person under 21 years of age is considered a minor.

Obtaining and Collecting Personal Data

The acquisition and collection of personal data must be based on the purpose(s) set out in the Privacy Notice and Consent. In other words, personal data must serve certain purposes as the basis for its collection. As an example, one's employer may require one's full name, address, contact number, and social security details. However, an employer should not require an employee's credit history or prior medical records, unless relevant. For example, an employer that operates a hazardous workplace, such as a steel mill, would most likely have a right to request medical records in the case of an employee who suffers from epilepsy.

Furthermore, the relevant sectoral government supervisory/regulatory agency may determine the type of personal data that is considered relevant and in accordance with the purposes of electronic system providers operating in their sector of responsibility. For example, the OJK, as the agency responsible for supervising the financial services sector, may determine which personal data is most relevant and in accordance with the purposes of the business operations of banks. The concept of involving the relevant sectoral agencies in determining what is and is not personal data is novel, if applied as intended.

However, it may make it more challenging to establish uniformity as to the meaning of personal data across the various sectors.

Personal data may only be acquired and collected based on prior consent, as expressly provided in the Privacy Notice and Consent. When providing prior consent, personal data owners have the right to stipulate that their personal data is confidential and may not be transferred or disclosed to third parties.

Storing Personal Data

The PDP Regulation provides a minimum retention period of 5 years for personal data, unless otherwise provided by a sector-specific regulation. This retention period is calculated from the time when the personal data owner terminates the use of the services provided by the electronic system provider. For example, if a person deletes an email address on 2 January 2017, any personal data related to that email address must be retained until 2 January 2022.

After the expiration of the said minimum retention period, the personal data may be erased, unless it is still to be used or utilized for the purpose that was originally consented to by the personal data owner.

Furthermore, the PDP Regulation requires personal data to be stored in the form of encrypted data. Even though this is not explained, encrypted data generally means data that is encoded in such a way that only authorized parties in possession of the encryption key can access it.

Displaying, Announcing, Transferring, Transmitting and Providing Access to Personal Data

Any display, announcement, transfer, distribution, or provision of access to personal data must be based on consent, as provided in the Privacy Consent and Notice. In addition, the accuracy of the personal data must first be verified. These requirements are applicable to actions conducted between electronic system providers, between electronic system providers and users, and between users.

As an example, in Facebook, generally a person will share his/her personal data with Facebook as well as other Facebook users (between electronic system providers and users, and between users). Using the same example, a Facebook account can usually be used to sign up for other services or platforms. In such a case, Facebook will share the personal data of their user who is signing up for the said other services or platforms, with the consent of the said user (between electronic system providers).

Data Centre for Public Services and Overseas Transfer of Personal Data

The data centre and disaster recovery centre for an electronic system that provides a public service must be located within the territory of Indonesia. Further details regarding this obligation will be provided by the sectoral regulator pursuant to (a) the respective laws and regulations, and (b) in coordination with the Minister.

An overseas transfer of personal data conducted by the Government or a private entity must be reported to the Minister of Communications and Information Technology. Reports must be submitted prior and subsequent to the transfer. The following aspects must be detailed in such reports:

1. Country of destination of the transfer;
2. Recipient of the transfer;
3. Date of the transfer; and
4. Reason for or purpose of the transfer.

Given that only providers of public services are required to maintain data centres and data recovery centres in Indonesia, the relevancy of these overseas transfer requirements might be questionable. With the prevalence of web based storage facilities and cloud services, it is increasingly common to view data storage as borderless.

Erasure of Personal Data

The erasure of personal data may be carried out in the following circumstances:

1. The retention period has elapsed based on the PDP Regulation, or a sector-specific regulation; or
2. Based on request from the personal data owner.

The erasure of personal data must be conducted thoroughly, covering both the deletion of electronic data and the destruction of non-electronic records, so that that the personal data can no longer be retrieved.

Obligations

The PDP Regulation imposes a comprehensive set of obligations on electronic system providers, including the following requirements:

1. to have their electronic systems certified;
2. to provide notification in case of a personal data breach;
3. to use legal software; and
4. to adopt internal policies for personal data protection.

Electronic System Certification

According to the PDP Regulation, an electronic system provider that manages personal data must have their electronic systems certified in accordance with the prevailing laws and regulations. This refers to Electronic System Worthiness Certification requirement under the Electronic Systems and Transactions Regulation, which is a process involving inspections and tests conducted by an authorized and competent institution to ensure that an electronic system is functioning properly. An Electronic System Worthiness Certificate may be issued by the Minister or an institution designed by the minister.

Under the Electronic Systems and Transactions Regulation, the Minister is required to issue an implementing regulation on the Electronic System Worthiness Certification process. However, as this regulation has not been issued to date, the provisions on Electronic System Worthiness Certification have yet to be implemented in practice.

Notification of Personal Data Breach

As also obligated by the Electronic Systems and Transactions Regulation, the PDP Regulation requires an electronic system provider to notify a personal data owner of any breach involving his/her personal data.

The notification may be provided in written or electronic form, depending on what was agreed under the Privacy Notice and Consent, and must give the reason for or cause of the personal data breach. It must be delivered to the personal data owner not more than 14 days subsequent to the occurrence of the breach. Further, the electronic system provider must ensure that it has been duly received if the breach has the potential to cause loss or damage to the personal data owner.

A failure to provide such notification provides the personal data owner with the right to submit an official complaint to the Minister.

Internal Data Protection Policy

An electronic system provider that manages or process personal data must develop and maintain an internal data protection procedure or policy for acquiring, collecting, processing, analysing, storing, displaying, announcing, transferring, transmitting, providing access to, and deleting personal data. This

internal policy must take into account such aspects as the applicable technology, human resources, technical procedures, and cost analysis, as well as be in accordance with the PDP Regulation and other prevailing laws and regulations.

The main purpose of adopting such internal policy is to prevent personal data breaches. The adoption of the policy must be accompanied by:

1. efforts to heighten the awareness of employees as to the importance of personal data protection; and

2. the provision of training for employees regarding the steps that must be taken to protect the personal data that is managed by the electronic system provider.

We believe the requirement to develop an internal policy represents a significant undertaking that electronic system providers, both in the public and private sectors, will have to face in the coming year.

Other Obligations

Other than the obligations described above, the PDP Regulation sets out a number of miscellaneous requirements that must be complied with by an electronic system provider that manages personal data:

1. To provide an audit trail record of all activities relating to the management of their electronic system;

2. To provide the option to choose whether or not personal data may be used and/or revealed to third parties;

3. To provide access to personal data owners to modify or update their personal data; and

4. To designate a contact person who can be easily reached.

Formal Complaints Procedure

A personal data owner or electronic system provider may lodge a formal complaint regarding a personal data protection breach with the Minister of Communications and Information Technology's Directorate General of Information Technology Application. The Directorate General will then initiate a consensual dispute resolution process between the parties in dispute.

Such formal complaint may be lodged pursuant to:

1. A failure on the part of an electronic system provider to provide a written notification of a personal data breach, whether or not this could potentially cause loss; or

2. Loss caused by a personal data protection breach because of delay on the part of the electronic system provider in providing written notification of the personal data breach.

The formal complaint must be lodged within 30 business days counting from the time when the prejudiced party discovered the personal data breach.

The official or team appointed to handle the complaint has 14 business days from the date of receipt of the complaint to state whether the complaint is complete and is supported by sufficient evidence. A complaint that is incomplete will be returned to the complainant, who will then have 30 business days to fulfil all the requirements.

Upon acceptance of the complaint, the dispute resolution process will be initiated within 14 business days. During this process, the official or team assigned to the handle the complaint may recommend to

the Minister of Communications and Information Technology that an administrative sanction be imposed on an electronic system provider that is involved, even if the dispute has yet to be resolved.

In the event that the dispute remains unresolved, the injured party may file a civil lawsuit against the electronic system provider in the local district court. If a seizure is required, the relevant law enforcement agency may only confiscate personal data that is relevant to the case, rather than seizing the entire electronic system.

Administrative Sanctions

Any person or legal entity found to be in violation of the PDP Regulation will be subject to the following administrative sanctions:

1. Verbal or written warning;
2. Temporary suspension of business activities; and/or
3. Public disclosure of the violation.

The procedures for imposing such administrative sanctions will be further provided for by the Minister of Communications and Information Technology.

Grace Period

The PDP Regulation gives existing electronic system providers 2 years (at most) to bring themselves into line with its provisions. The most significant adjustments that will need to be made are as follows:

1. Preparing a Privacy Notice and Consent form;
2. Encrypting personal data that is stored;
3. Reporting overseas transfers of personal data to the Minister of Communications and Information Technology (if applicable);
4. Certifying electronic systems used to manage personal data (once the necessary procedures have been put in place by the Minister);
5. Establishing an internal policy for personal data protection;
6. Providing an audit trail record of all activities relating to the management of an electronic system;
7. Providing access to personal data owners to modify or update their personal data; and
8. Designating a contact person who can be easily reached.

Contacts

Eko Ahmad Ismail Basyuni
Partner
Mergers & Acquisitions

D (62) 21 2555 7802
F (62) 21 2555 7899
eko.basyuni@ahp.co.id

Zacky Zainal Husein
Partner
Mergers & Acquisitions

D (62) 21 2555 9956
F (62) 21 2555 7899
zacky.husein@ahp.co.id

ASEAN Economic Community Portal

With the launch of the ASEAN Economic Community ("**AEC**") in December 2015, businesses looking to tap the opportunities presented by the integrated markets of the AEC can now get help a click away. Rajah & Tann Asia, United Overseas Bank and RSM Chio Lim Stone Forest, have teamed up to launch "Business in ASEAN", a portal that provides companies with a single platform that helps businesses navigate the complexities of setting up operations in ASEAN.

By tapping into the professional knowledge and resources of the three organisations through this portal, small- and medium-sized enterprises across the 10-member economic grouping can equip themselves with the tools and know-how to navigate ASEAN's business landscape. Of particular interest to businesses is the "Ask a Question" feature of the portal which enables companies to pose questions to the three organisations which have an extensive network in the region. The portal can be accessed at http://www.businessinasean.com/.

Our regional presence

Our regional contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
9 Battery Road #25-01
Straits Trading Building
Singapore 049910
T +65 6535 3600 F +65 6225 9630
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
Vattanac Capital Office Tower, Level 17, No. 66
Preah Monivong Boulevard, Sangkat Wat Phnom
Khan Daun Penh, 12202 Phnom Penh, Cambodia
T +855 23 963 112 / 113 F +855 963 116
kh.rajahtannasia.com
**in association with Rajah & Tann Singapore LLP*

RAJAH & TANN REPRESENTATIVE OFFICE | *China*

Rajah & Tann Singapore LLP
Shanghai Representative Office
Unit 1905-1906, Shui On Plaza, 333 Huai Hai Middle Road
Shanghai 200021, People's Republic of China
T +86 21 6120 8818 F +86 21 6120 8820
cn.rajahtannasia.com

RAJAH & TANN NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
Myanmar Centre Tower 1, Floor 07, Unit 08,
192 Kaba Aye Pagoda Road, Bahan Township,
Yangon, Myanmar
T +95 9 73040763 / +95 1 657902 / +95 1 657903
F +95 1 9665537
mm.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office
Menara Rajawali 16th Floor
Jalan DR. Ide Anak Agung Gde Agung Lot #5.1
Kawasan Mega Kuningan, Jakarta 12950, Indonesia
T +62 21 2555 7800 F +62 21 2555 7899
www.ahp.co.id

Surabaya Office
Pakuwon Center, Superblok Tunjungan City
Lantai 11, Unit 08
Jalan Embong Malang No. 1, 3, 5, Surabaya 60261, Indonesia
T +62 31 5116 4550 F +62 31 5116 4560

** Assegaf Hamzah & Partners is an independent law firm in Indonesia and a member of the Rajah & Tann Asia network.*

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
Level 22, Axiata Tower, No. 9 Jalan Stesen Sentral 5,
Kuala Lumpur Sentral, 50470 Kuala Lumpur, Malaysia
T +60 3 2273 1919 F +60 3 2273 8310
www.christopherleeong.com
**in association with Rajah & Tann Singapore LLP*

RAJAH & TANN | *Thailand*

Rajah & Tann (Thailand) Limited
973 President Tower, 12th Floor, Units 12A-12F
Ploenchit Road, Lumpini, Pathumwan
Bangkok 10330, Thailand
T +66 2 656 1991 F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Sole Co., Ltd.
Phonexay Village, 23 Singha Road, House Number 046/2
Unit 4, Saysettha District, Vientiane Capital, Lao PDR
T +856 21 454 239 F +856 21 285 261
la.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
Saigon Centre, Level 13, Unit 2&3
65 Le Loi Boulevard, District 1, HCMC, Vietnam
T +84 8 3821 2382 / +84 8 3821 2673 F +84 8 3520 8206

Hanoi Office
Lotte Center Hanoi - East Tower, Level 30, Unit 3003,
54 Lieu Giai St., Ba Dinh Dist., Hanoi, Vietnam
T +84 4 3267 6127 F +84 4 3267 6128
www.rajahtannlct.com

Based in Jakarta, and consistently gaining recognition from independent observers, Assegaf Hamzah & Partners has established itself as a major force locally and regionally, and is ranked as a top-tier firm in many practice areas. Founded in 2001, it has a reputation for providing advice of the highest quality to a wide variety of blue-chip corporate clients, high net worth individuals, and government institutions.

Assegaf Hamzah & Partners is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, Thailand and Vietnam. Our Asian network also includes Singapore-based regional desks focused on Japan and South Asia.