Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Indonesia
SSEK Legal Consultants

chambers.com

2019

Law and Practice

Contributed by SSEK Legal Consultants

Contents

SSEK Legal Consultants specialise in: banking and finance; consumer goods and retail; healthcare; hotels and tourism; insurance; labour and employment; telecommunications, media and technology. SSEK's telecommunications and IT practice, which includes its data protection team, has 15 members. Its award-winning labour and employment practice has 20 members and advises corporate clients on data protection matters as they relate to the collection, use and storage of employee data. The data protection team works with SSEK's corporate acquisitions and mergers practice to advise on data protection law in Indonesia. The firm's banking and finance practice has 15 members and advises clients on the collection, use and storage of customer data. SSEK's data protection team works with the firm's ten-strong health practice to advise on data protection rules in Indonesia related to the collection and use of patient data. Two of the firm's partners – Denny Rahmansyah and Fahrul S Yusuf – were contacted last year and interviewed in relation to articles on the data privacy scandal involving Facebook, in which more than one million Indonesian Facebook users were affected.

Authors

Denny Rahmansyah is managing partner of the firm. His key practice areas are IT and telecommunications, including extensive experience advising clients on data privacy and data protection regulations in Indonesia, banking and finance, foreign investment, general commercial and corporate law, M&A, real estate and property. Denny has advised several multinationals and Fortune 500 companies on data protection and data privacy issues. Last year, Denny was quoted extensively in an article by MLex Market Insight, a subscription-only service that analyses regulatory risk around the world.

Farah Nabila is an associate of the firm. Her key practice areas are data protection, foreign investment, general corporate law, and M&A.

1. Basic National Legal Regime

1.1 Laws

The fundamental basis for privacy and data protection in Indonesia can be found in Article 28(G) of the 1945 Constitution of the Republic of Indonesia, which provides that every person has the right to:

- protection of themselves, their families, respect, dignity and possessions under their control; and
- security and protection from threat of fear for doing, or not doing, something that constitutes a human right.

To date, there is no specific law in Indonesia that regulates protection of private and family life. The most relevant regulation for the protection of privacy is related to personal data protection.

Provisions on the protection of personal data can be found in 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'). The procedural guidelines for the Electronic Information Law are contained in Government Regulation No 82 of 2012 regarding the Implementation of Electronic Systems and Transactions (27 February 2012) ('Government Regulation 82'). However, none of these regulations provides a comprehensive set of provisions for the protection of personal data, but rather, simply the general idea of personal data protection without specific guidelines. On 1 December 2016, the Ministry of Communication and Informatics (MOCI) issued a regulation specifically for the protection of personal data that is contained in an electronic system, namely MOCI Regulation No 20 of 2016 regarding the Protection of Personal Data in Electronic Systems (1 December 2016) ('MOCI Regulation 20'). MOCI Regulation 20 is an implementing regulation for the Electronic Information Law and Government Regulation 82. The Electronic Information Law, Government Regulation 82 and MOCI Regulation 20 are jointly referred to here as the PDP Regulations.

The application of the PDP Regulations appears to be rather broad. This can be seen from the definition of Electronic System Providers (ESP) under the PDP Regulations, which covers every person, state administrator, business entity and community providing, managing, and/or operating an electronic system, either individually or jointly, for electronic system users, for their personal purpose and/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 and/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.

1.2 Regulators

The key regulator for data protection in Indonesia is the MOCI. Officials at the ministry supervise the implementation of the PDP Regulations, particularly MOCI Regulation 20.

To implement its supervisory role, the relevant official at the MOCI is authorised to request any data and information from an ESP to ensure its compliance with data protection rules. This may be done periodically or at any time considered necessary.

In the event of a dispute, the MOCI may delegate its authority to settle the dispute to its Director General of Informatics Application (the 'Director General'), who will form a data privacy dispute settlement panel. This panel may provide a recommendation to the MOCI to impose administrative sanctions against the relevant ESP, although the dispute can also be settled amicably or by any other alternative dispute resolution process between the ESP and the owner of the data.

As for cyber-security, the Indonesian Police has formed a cyber-crime unit dedicated to investigating online crimes.

1.3 Administration and Enforcement Process

The MOCI can only commence an investigation after receiving a complaint from a data subject and/or ESP. The complaint can be filed on the grounds that a data breach exists. The dispute will then be settled by the data privacy dispute settlement panel formed by the Director General, with all the parties involved.

As there are no clear standards or criteria for the threshold of the 'loss' caused by the data breach, disputes are settled on a case-by-case basis. The PDP Regulations do not provide any right to appeal the conclusion of this dispute settlement panel.

1.4 Multilateral and Subnational Issues

While the PDP Regulations are intended to have extraterritorial jurisdiction, the Indonesian national system relating to personal data protection is in no way related to any multinational system, such as the EU or APEC. Neither Asian nor ASEAN countries have any particular joint governance relating to personal data protection.

Aside from the PDP Regulations, which apply nationally, there are no other regulations, particularly at the regional level, relating to data protection and cyber-security.

1.5 Major NGOs and Self-Regulatory Organisations

To the best of our knowledge, there are no non-governmental organisations (NGOs) or industry self-regulatory organisations (SROs) established specifically for data protection-related matters. Nevertheless, there are a number of civil society organisations, such as SAFEnet (Southeast Asia Freedom of Expression Network) and a number of Community Legal Aid Institutes ('Lembaga Bantuan Hukum Masyarakat') that have been active in scrutinising and criticising the development and content of the new PDP Draft Law, see **1.8 Significant Pending Changes, Hot Topics and Issues**.

1.6 System Characteristics

It is important to highlight that the concept of data protection is generally new in Indonesia. The relevant regulations are still developing and there has been much discussion and effort to broaden and strengthen protections to a level comparable with what is found in developed countries, such as the EU model. That said, while the Indonesian government has strongly urged ESPs to implement rights and obligations under the PDP Regulations, the supervision and enforcement of applicable sanctions has not been particularly proactive.

1.7 Key Developments

The past 12 months has seen growing public awareness of the power of the PDP Regulations. A large number of people have filed police complaints for defamation of character or malicious comments made on social media.

Aside from the above, one of the major highlights of 2018 was the criminal investigation initiated by the police in response to the dissemination of a hoax by a well-known activist in Indonesia during the presidential election cycle. The activist, a spokeswoman for one of the presidential candidates, claimed on a social messaging application that she had been assaulted by supporters of the opposing presidential candidate. This hoax received substantial attention and caused public outrage, prompting the police to open a criminal investigation for violation of the Electronic Information Law for the dissemination of false information. The activist in question was arrested by the police for further investigation.

1.8 Significant Pending Changes, Hot Topics and Issues

It has been rumoured that the Indonesian House of Representatives is in the process of discussing a draft law on personal data protection (the 'PDP Draft Law'). Based on media reports, the PDP Draft Law is on track for issuance by the end of 2019. If enacted, the PDP Draft Law would be the first comprehensive law in Indonesia to specifically deal with the protection of personal data. The current draft seems to include several provisions similar to those found in vari-

ous jurisdictions that give individuals more control of their online information.

There has also been an effort to amend Government Regulation 82 (the 'Draft Amendment of GR 82'). It appears that the Draft Amendment of GR 82 introduces several categories of data that do not exist in Government Regulation 82, such as strategic electronic data, high-risk electronic data and low-risk electronic data, all of which would trigger different levels of responsibility for the ESP.

The two aforementioned drafts are 'live' drafts and still subject to further changes. Therefore, it cannot be guaranteed that the changes discussed above will be included in the final drafts.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

As a civil law country, Indonesia has not applied the concept of omnibus laws. All of the requirements pertaining to data protection are covered by the PDP Regulations.

It is assumed that the concept of a privacy or data protection officer generally refers to authorised person(s) who shall supervise, investigate and determine the applicable sanctions for any party that violates data protection obligations. Under the PDP Draft Law, such authority is granted to the MOCI, which may receive complaints or reports from the public and then investigate and sanction ESPs that do not comply with their obligations.

The PDP Draft Law only provides a general requirement that the consent of the data subject be obtained to authorise the collection, use or other processing of any data.

A law enforcement officer may be exempted from the requirement to obtain the consent of the data subject in the event that they wish to seize the relevant data for investigation purposes. However, in these circumstances only data relevant to the matter of the investigation can be seized. During the course of the investigation the ESP storing such data is still obligated to protect the safety and confidentiality of such data.

The PDP Regulations have not introduced the concept of 'privacy by design' or 'by default.'

The PDP Regulations do not require ESPs to conduct privacy impact analyses.

The PDP Regulations require ESPs to adopt an internal policy related to the protection of personal data for the purpose of, including but not limited to, acquiring, collecting, processing, analysing, storing, dissemination, transmission and destruction of data. This internal policy shall be drafted as a means to prevent any failure in the protection of data in their system.

With regard to access, data subjects are granted the right to:

- obtain access or the opportunity to change or update their personal data without interfering with the personal data management system, unless otherwise provided by applicable laws and regulations;
- obtain access or the opportunity to receive the history of their personal data that has been given to the ESP insofar as it is still in accordance with the applicable laws and regulations; and
- request the destruction of their personal data in an electronic system managed by the ESP, unless otherwise determined by the applicable laws and regulations.

The PDP Regulations do not govern the use of data pursuant to anonymisation, de-identification, or pseudonymisation.

Restrictions on or allowances for profiling, automated decision-making, online monitoring or tracking, Big Data analysis and artificial intelligence do not exist in the current PDP Regulations.

The existing PDP Regulations provide for 'loss' – which can be loosely translated as 'injury' or 'harm' – as a ground to file a complaint of an alleged data breach (see section 41). However, the PDP Regulations do not define the scope of the term 'loss' for this purpose. The scope of this 'loss' is specified in the PDP Draft Law not only to include material loss, but also morale loss, such as defamation of one's or an organisation's character.

2.2 Sectoral Issues

The PDP Regulations do not provide specific definitions of sensitive data, and consequently no special issues apply. There are, however, several laws in a number of specific areas that indirectly deal with data privacy relating to financial, health and communications data.

Financial service providers are prohibited by Article 31 of Financial Services Authority ('Otoritas Jasa Keuangan' or 'OJK') Regulation no 1/POJK.07/2013 regarding financial consumer protection (6 August 2013) ('POJK no 1/2013') from disclosing customer data and/or information to third parties, unless they receive written consent from the customer or are required to by lawful authority. If a financial service-provider obtains the personal data and/or information of a person and/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.

Additionally, the protection of consumers' personal data and/or information in relation to the payment transaction process conducted by payment service providers is provided for under Article 25 of Bank Indonesia Regulation no 18/40/PBI/2016 regarding the provision of payment transaction processing (9 November 2016).

Article 57 of 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.

Article 40 of Law No 36 of 1999 regarding telecommunications (8 September 1999) prohibits the 'tapping' of information transmitted through telecommunications networks. Telecommunications service operators must keep confidential any information transmitted, and/or received by a telecommunications service subscriber, through a telecommunications network and/or telecommunications services provided by the relevant operator.

As specified above, the PDP Regulations do not contain any provision regarding sensitive data. This will likely be included in the Draft PDP Law.

To date, there is no regulation pertaining to any rights and/or obligations for text messaging.

There exists an obligation for telecommunications service operators to maintain the confidentiality of all data transmitted and/or received by their systems.

There is no specific regulation in Indonesia governing internet activities. Most provisions regarding rights and obligations related to the internet are found in the Electronic Information Law, which is part of the PDP Regulations.

There is a general obligation for an ESP to adopt an internal privacy policy. Due to the broad definition of ESP, this would also include internet operators. The regulations, however, do not provide any details on the provisions that must be included in such a privacy policy. See **2.1 Omnibus Laws and General Requirements**.

The Electronic Information Law does not regulate any requirements or prohibitions regarding the use of cookies, beacons or tracking technology.

The PDP Regulations, including the Electronic Information Law, do not include 'do not track' considerations as a step that data subjects can take to protect their personal information.

The existing PDP Regulations do not have specific provisions regarding behavioural advertising. However, as a general rule, all activities related to the processing of personal data are allowed insofar as the processor has duly obtained the consent of the data subject. Therefore, it is safe to assume that behavioural advertising is allowed, insofar as the data subject whose data is used as the basis for such advertising has provided their consent.

The PDP Regulations do not provide specific provisions regarding video and television, instead categorising them all as one 'electronic document.'

In the absence of any specific regulatory obligations for social media, search engines and large online platforms, the obligations of ESPs under the PDP Regulations shall apply for activities conducted on such platforms.

A data subject is entitled to request the deletion of their personal data, provided that such request is conducted in accordance with the applicable laws and regulations. Nevertheless, there is currently no regulation that specifically governs procedures to request such deletion and subsequent follow-up actions.

The Electronic Law prohibits any person, either deliberately or otherwise, from distributing and/or transmitting and/or making accessible electronic information and/or electronic documents with materials that may spread hatred against individuals and/or groups based on culture, religion, race or community, or materials that are:

- inappropriate;
- gambling-related;
- insulting and/or defamatory;
- extortive and/or threatening; or
- hoaxical or misleading and which may result in losses to the customer.

The PDP Regulations give data subjects the right to obtain access to the history of their personal data that has been given to any ESP insofar as it is still in accordance with the applicable laws and regulations. Similar to the right to be forgotten, no implementing regulations have as yet been issued specifying the steps to be taken by data subjects to exercise this right.

If a data subject is a child or considered to be a minor, the general requirement of consent can be provided by the data subject's parents or rightful guardian, in accordance with the applicable laws and regulations. The parents must be either the biological father or mother, while the guardian must be the person who has a lawful obligation to care for the child.

Despite a certain ambiguity in the age of maturity in Indonesia, it is widely accepted that a person can be considered to be of legal age at age 18.

There are no specific regulations pertaining to educational or school data.

2.3 Online Marketing

The PDP Regulations are silent on the sending of unsolicited commercial or marketing communications.

While it is not explicit, the Financial Services Authority, through its POJK no 1/2013, has imposed a prohibition on telemarketing telephone calls or texts by prohibiting businesses in the financial services sector from making any product or service offering or marketing to consumers and/or the public through private communication facilities without the prior consent of the consumer. Businesses in the financial services sector are defined as commercial banks, rural banks, securities companies, investment advisors, custodian banks, pension funds, insurance companies, reinsurance companies, multi-finance institutions, pawn companies and guarantee companies that operate under conventional or sharia arrangements. The Regulation also specifies that the business must include and/or mention the logo and/or the name of its company and a statement that it is duly registered and supervised by the OJK. Consumers can file a complaint with the OJK if they receive telemarketing telephone calls or texts, and the OJK will proceed to investigate and stipulate any applicable sanctions for such business. The sanctions range from a written warning and fines to the limitation of business scope, suspension of business activities, and revocation of its business licence.

There are no specific regulations pertaining to behavioural advertising. As such, the activity of behavioural advertising is subject to the general requirement for the obtainment of consent of the data subject.

There are no specific regulations pertaining to location-based advertising or other communications. As such, the activity of location-based advertising is subject to the general requirement for the obtainment of consent of the data subject.

2.4 Workplace Privacy

No special laws or considerations apply to workplace privacy in Indonesia. It is generally considered sufficient for employers in Indonesia to regulate the protection of the personal data of their employees by way of unilateral employee consents, employment agreements, company regulations and collective labour agreements.

In the absence of particular provisions regarding workplace privacy, constraints generally include the applicable privacy rules, rooted in the consent of the data subject. As such, even in the workplace, an employer should ensure that it does not intercept private conversations without the consent of the employee, aside from professional communications in the workplace.

Labour organisations or work councils are recognised as labour unions in Indonesia. A labour union is an organisation that is formed by and for the workers/labour in a company or outside of a company in order to protect the rights and interests of workers/labour. Through a labour union, workers are expected to be able to communicate their criticisms and demands of a company, to be further realised in a collective agreement between employees and the management of the company. While such communications allow workers to discuss the implementation of workplace policy, most matters brought up by labour unions deal with unfair termination and/or payment of services.

We are not aware of any whistle-blower hotlines or anonymous reporting venues for workplace privacy-related matters.

2.5 Enforcement and Litigation

The PDP Regulations do not provide much detail on the standards that must be established by regulators to allege violations of privacy or data protection laws. In the absence of specific standards, in order to allege violations of privacy or data protection laws, a regulator is bound by the standards under the applicable criminal laws in Indonesia. Indonesian criminal law requires a regulator to put forward a minimum of two pieces of evidence in order to establish an allegation of any criminal violation. Under the Electronic Information Law, any electronic document would constitute lawful evidence.

The Electronic Information Law provides for criminal penalties including:

- fines of IDR600 million to IDR800 million and/or four to eight years' imprisonment for unlawful access;
- fines of IDR800 million to IDR1 billion and/or six to ten years' imprisonment for interception/wiretapping of transmission;
- fines of IDR2 billion to IDR5 billion and/or eight to ten years' imprisonment for the alteration, addition, reduction, transmission, tampering, deletion, moving or hiding of electronic information and/or electronic records; and
- fines of IDR10 billion to IDR12 billion and/or ten to 12 years' imprisonment for the manipulation, creation, alteration, destruction or damage of electronic information and/or electronic documents with the purpose of creating an assumption that such electronic information and/or documents are authentic, and other violations related to the processing of electronic information and/or documents.

Government Regulation 82 provides administrative sanctions – that do not abrogate any civil and criminal liability – in the form of written warnings, administrative fines, temporary dismissal of part of the components or services in the related electronic system for a certain period, and exclusion

from the list of registrations of ESP (as required under the regulation).

For any party processing personal data without lawful authority or at odds with the laws and regulations, MOCI Regulation 20 provides administrative sanctions in the form of verbal warnings, written warnings, temporary dismissal of activities and an announcement on MOCI's website stating that the party has not complied with data protection regulations.

The cybercrime unit of the Indonesian Police has become quite aggressive in investigating cybercrimes pertaining to malicious comments, defamation of character and hoaxes, particularly those that interfere with the national interest. One of the most recent highest-profile enforcement cases relating to cybercrime involved Buni Yani, a former lecturer at a private university in Jakarta, who was convicted of violating Article 32 of the Electronic Information Law, for editing an electronic document so that the altered document was publicly accessible. The case was opened following a public outcry over Buni editing a video of a speech given by a gubernatorial candidate to make it appear the candidate had committed an act of blasphemy, and then uploading the video to the internet. The prosecution in the case presented several electronic documents as evidence, namely a screenshot of Buni's social media account, his email account, mobile phone and the video that had been uploaded to the internet. The defendant was sentenced to 18 months in prison.

In 2013, a 19-year-old man was sentenced to six months in prison and fined after he was found guilty of hacking the official website of a former president of Indonesia. Another hacker was sentenced to 15 months in prison after he was found guilty of hacking the official website of the Indonesian Press Council.

The Electronic Information Law allows any violation of the PDP Regulations to be resolved privately through a civil suit, in accordance with the applicable laws and regulations. Generally, a civil suit can be filed based on one of two grounds – namely, a breach of contract or an unlawful act. Specifically, for unlawful acts, the plaintiff must prove that the defendant has committed an unlawful act in contrary to the laws and regulations, causing a loss to the plaintiff. There must also be a causal link between the unlawful act and the losses suffered by the plaintiff.

There are no express provisions for class actions over data protection and/or cybersecurity violations, as are available under the Indonesian Environmental Law and Consumer Protection Law. It is unknown if there has ever been an attempt to file a class action suit for violations of data protection and cybersecurity.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

There are no specific regulations in Indonesia regarding the stipulation of serious crimes and therefore a lack of guidance for the particular procedures applicable to the investigation of or law enforcement access for serious crimes. In such situation, it is assumed that general Indonesian procedural criminal law shall apply.

Under the Indonesian Criminal Law, an investigator or any other authorised officer shall obtain judicial approval before they raid a private premise/space or (forcefully) access personal data or any other confidential data for investigation purposes. Such judicial approval can be obtained after the completion of such raid or access if there exists a compelling reason to do so. It is expected that this procedure would similarly be applied in the case of serious crimes.

3.2 Laws and Standards for Access to Data for National Security Purposes

The general Indonesian procedural criminal law shall apply in these circumstances.

3.3 Invoking a Foreign Government

The PDP Regulations are silent on any privilege for a foreign government to access, collect and transfer personal data. It is presumed that an organisation cannot invoke a foreign government access request as a basis to collect and transfer personal data without the consent of the data subject, unless such foreign government has entered into a separate co-operation with the Indonesian government relating to the matter. The organisation, as an ESP, in this case, is also subject to the transfer data notification requirement, as discussed in section **4.1 Restrictions on International Data Issues** below.

3.4 Key Privacy Issues, Conflicts and Public Debates

There has been debate about the extended authority of Indonesia's Corruption Eradication Commission, a government agency established to fight corruption, and other government institutions to wiretap/intercept communications for the purpose of an investigation. On one side of the debate are those who fear that the broad and ambiguous circumstances that allow such institutions/officials to wiretap/intercept communications could be abused so as to intercept communications of any civil servant, even when the situation does not call for it. On the other side, the Corruption Eradication Commission argues such power is necessary and has contributed to its high rate of success in prosecuting corruption cases. Indonesia's House of Representatives is now in the process of drafting a new Interception/Wiretapping Law to regulate the circumstances and procedures

for the interception/wiretapping of communications. One of the key provisions in the draft law requires the Corruption Eradication Commission to obtain prior judicial approval before conducting such activity. The draft law is still being discussed and is thus subject to change.

4. International Considerations

4.1 Restrictions on International Data Issues

MOCI Regulation 20 requires that the transfer of data overseas be carried out in co-ordination with the Ministry of Communication and Informatics. This co-ordination entails:

- reporting the plan to transfer the personal data. As a minimum, the report must include the name of the destination country; the name of the receiving party; the date of the transfer; and the reason for/purpose of the transfer;
- requesting the assistance of the MOCI for the transfer (if required); and
- reporting the result of the transfer activity.

The MOCI has not, however, specified the procedures to implement this coordination, and very few businesses are known to have, of their own volition, attempted to comply with the co-ordination obligation. The MOCI has never sought to enforce the rule, which for the time being is widely disregarded in practice.

MOCI Regulation 20 further stipulates that the transferring entity would need to apply the laws and regulations on the cross-border country exchange of personal data. However, since Indonesia has yet to issue any laws or regulations on the subject, it is currently not possible for an ESP to comply with this requirement. As a result, ESPs are not, in practice, required to fulfil this obligation.

4.2 Mechanisms That Apply to International Data Transfers

See section **4.1 Restrictions on International Data Issues** above. There is currently no additional mechanism that must be applied to international data transfers.

4.3 Government Notifications and Approvals

See **4.1 Restrictions on International Data Issues** above.

4.4 Data Localisation Requirements

The PDP Regulations require an ESP engaged in public services to have a data centre and disaster recovery centre located within the jurisdiction of the Republic of Indonesia, but do not specify the types of data that must be on-shored.

The Draft Amendment of GR 82 limits the obligation for data localisation to data that falls under the category of strategic electronic data. Under the draft amendment of GR 82, strategic electronic data means data with a strategic impact on public interest, public service, smooth governance of the state, or state defence and security. Elucidation of the relevant article provides an example of such strategic electronic data, namely "intelligence data, demographic data, or data of Indonesian citizens, data on national defence and security." Such data must be managed, processed and stored in the territory of Indonesia, while other types of data that fall outside the definition of strategic data may be processed and stored outside the territory of Indonesia. It remains to be seen whether the final amendment of GR 82 will adopt this view.

There is no prohibition under the PDP Regulations or any other laws on the cross-border transfer of data that is required to be maintained in-country, provided that the transfer of the data is conducted pursuant to the PDP Regulations.

4.5 Sharing Technical Details

There is no obligation under the PDP Regulations or any other prevailing laws to share any software code or algorithms or similar technical detail with the government, unless such information is required for law enforcement purposes.

4.6 Limitations and Considerations

There are no limitations or considerations that may be applied to an organisation collecting or transferring data in connection with foreign government data requests, foreign litigation proceedings or internal investigations, as long as it is conducted in accordance with the applicable laws and regulations. We are not aware of any blocking statutes implemented by the government of Indonesia, particularly relating to privacy or data protection.

4.7 "Blocking" Statutes

See **4.6 Limitations and Considerations** above.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

As stated above, the PDP Regulations in Indonesia are relatively new and still under development. The current PDP Regulations do not touch upon such issues as Big Data, automated decision-making, Artificial Intelligence (AI), Internet of Things (IoT) and the like, and therefore there is still a major void when it comes to data protection in such circumstances. The latest Draft PDP Law discusses more complicated issues such as biometric data as sensitive data subject to particular treatment. However, the Draft PDP Law is still being discussed and the final contents of the law cannot yet be confirmed.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators

The Indonesian legal framework for cybersecurity is varied, depending on the context of the crime. However, the main reference would be the PDP Regulations, which broadly discuss the privacy of personal data and electronic communications. Aside from the PDP Regulations, there are other key laws regarded as the basis for cybersecurity. For example, with regard to intellectual property, the Ministry of Law and Human Rights, along with the MOCI, jointly issued Decree no 14 of 2015 and no 26 of 2015 (2 July 2015) regarding the Implementation of Closing Down Content and/or a User's Right to Access over Copyright Infringement and/or Related Rights in an Electronic System. The joint decree elaborates the procedure to file a report on copyright infringement in an electronic system, the verification procedure for reports, and the procedure for closing down content and/or access rights pertaining to copyright infringement.

The MOCI is considered the key regulator for matters relating to data protection and cyber activities, while the police has formed its own unit to handle cybercrimes. For further explanation on this point, see section 2.

In addition to the above, the government has established other bodies specifically to oversee cybersecurity and IT security, namely the Cyber Body and National Encryption Agency ('Badan Siber dan Sandi Negara' or 'BSSN') and the Indonesia Security Incident Response Team on Internet and Infrastructure (ID-SIRTII).

The Financial Services Authority ('Otoritas Jasa Keuangan' or 'OJK') is also regarded as a key regulator for any matter relating to the protection of the personal data and/or information of consumers in relation to the payment transaction process or general financial service activities:

- Identify what laws apply to what data, systems, infrastructure, etc.
- Identify what regulators are responsible for what cybersecurity areas.
  - (a) Discuss any over-arching cybersecurity agency (e.g., ENISA).
  - (b) Discuss the role of data protection authorities or privacy regulators.
  - (c) Discuss role of financial or other sectoral regulators.
  - (d) Discuss other key relevant regulators and agencies.

6.2 Key Frameworks

MOCI Regulation no 4 of 2016 regarding Information Security Management Systems (11 April 2016) in essence imposes the obligation for the mandatory application of SNI ISO/EIC 27001. The Regulation divides electronic systems for public services into three categories based on their risks. These categories are:

- strategic electronic systems, being systems that have a serious impact on public interest and services, state administration continuity, or national security and defence;
- high-level electronic systems, being systems with a limited impact on sectoral and/or regional interests; and
- low-level electronic systems.

Systems considered as strategic and high-level must implement the SNI ISO/EIC 27001 standard and obtain an Information Security Management Certificate from a certification institution acknowledged by the MOCI.

The adoption of SNI ISO/EIC 27001 is supported by the assumption that an ESP that passes SNI ISO/EIC 27001 is guaranteed to be able to protect the security and confidentiality of personal data. Despite being mandatory only for governmental entities, other private ESPs, including major private banks and start-up technology companies, have completed their SNI ISO/EIC 27001 certification.

6.3 Legal Requirements

There are no specific legal requirements and applicable standards relating to cybersecurity matters, other than for the banking and financial sectors. Companies in the banking and financial sectors have the obligation to designate a chief information security officer, submit an incident response plan, conduct periodic assessments of their staff and technology service providers, and perform a simulation of their disaster recovery plan.

6.4 Key Multinational Relationships

The Indonesian National Police has entered into agreements with other countries including Australia and the United States to mitigate cybercrimes and improve the capacity of its personnel.

Police officers from Indonesia have attended courses on cybercrime at the Australia-backed Jakarta Centre for Law Enforcement Cooperation.

The co-operation between the Indonesian National Police and the United States Attorney General's Office began after the adoption of the ASEAN-US Leaders' Statement on Cybersecurity Cooperation, a cybersecurity pact between the regional bloc and the United States to fight cybercrime and cyberattacks.

With renewed anxieties over the threat of cyberattacks and terrorism, the ASEAN nations have also vowed to increase co-operation with other countries including Australia, China, India, Japan, South Korea, New Zealand and Russia.

6.5 Data Breach Reporting and Notification

In the event of a data breach or failure to protect the confidentiality of the personal data stored in the related ESP's

system, the ESP must provide a notification to the data subject with the reason or cause of the failure to protect the confidentiality of the personal data. The notification may be sent electronically if the data subject approved such electronic notification during the acquisition and collection of their personal data. The ESP must ensure that the notification has been received by the data subject if the data breach has the potential to cause loss to the relevant data subject. The written notification must be sent to the data subject no later than 14 days after the identification of the breach. In addition, although there is no legal requirement to notify such data breach to the government, the MOCI has verbally stated on multiple occasions that it expects an ESP to notify it of any data breach as well, but failure to do so will not result in any sanction.

Similarly, every data subject can file a complaint to the MOCI if no notification of the data breach is given, or a loss has occurred to the data subject as a result of such data breach. This is intended as an effort to resolve a dispute by deliberation or through other alternative resolution efforts. There is no clear standard or threshold of the expected loss that may give rise to such entitlement, and therefore it must be assessed on a case-by-case basis.

6.6 Ability to Monitor Networks for Cybersecurity

Indonesia permits the practice of communications wiretapping/interception, if it is done by an authorised law enforcer for the purpose of law supremacy and national security. This communications wiretapping, nevertheless, is only authorised to be conducted by five key regulators – the police, prosecutors, and officials from the Corruption Eradication Commission, National Anti-Narcotics Agency, and the National Intelligence Agency. Such authority shall be used for limited purposes only; that is for law enforcement. Such wiretapping activity must be done in close cooperation with the relevant telecommunications operators.

SSEK Legal Consultants

14th Floor, Mayapada Tower
Jl Jend Sudirman Kav 28
Jakarta 12920
Indonesia

Tel: +62 21 5212038
Fax: +62 21 5212039
Email: ssek@ssek.com
Web: www.ssek.com

Furthermore, possession of cybercrime tools is allowed if the tools are intended for research activities, testing and protection of the relevant electronic system, insofar as the tools were obtained in a lawful manner.

6.7 Cyberthreat Information Sharing Arrangements

Aside from the requirement to report on the plan to transfer data (see section 28), the PDP Regulations do not provide any required or authorised sharing of cybersecurity information with the government. In any event, the Indonesian Criminal Law generally requires any person who has information about the occurrence or potential occurrence of a crime to report such knowledge to the police or other authorised officer. Due to the broad application of this requirement, there is a general requirement to share any cybersecurity information with the police or other authorised officials.

The PDP Regulations provide several voluntary information sharing opportunities with the MOCI, in the event of:

- any failure to protect the confidentiality of the personal data stored in the related ESP's system;
- any failure to submit/receive a data breach notification due to the failure to protect personal data; and
- any failure or disruption of a system that may have a serious impact, as a result of a third party's actions (in which case the ESP must secure the data and report the situation in the first instance to the authorised official).

6.8 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

Enforcement actions are normally taken pursuant to business sectors. An insurance company in Indonesia has been known to have received a warning letter from the Financial Services Authority in relation to the obligation to open a data centre in Indonesia. However, a case has yet to be seen where the failure to meet compliance requirements for data protection and cybersecurity resulted in the imposition of administrative fines or suspension of business activities.