COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

Indonesia

DATA PROTECTION & CYBER SECURITY

Contributing firm

Bagus Enrico & Partners (BE Partners)

Enrico Iskandar

Founding Partner | enrico@bepartners.co.id

Bratara Damanik

Principal Associate | bratara@bepartners.co.id

Alwin Widyanto Hartanto

Associate | alwin@bepartners.co.id

This country-specific Q&A provides an overview of data protection & cyber security laws and regulations applicable in Indonesia.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

INDONESIA
DATA PROTECTION & CYBER SECURITY

1. Please provide an overview of the legal and regulatory framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws)?

The general concept of 'data protection' are dispersed within various regulation including Law No. 11 of 2008 on Electronic Information and Transaction as lastly amended by Law No. 19 of 2016 ("**EIT Law**"), Government Regulation No. 71 of 2019 on the Implementation of the Electronic System and Transaction ("**GR 71/2019**"),and the Ministry of Communications and Informatics ("**MCI**") Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic System ("**MCI Regulation 20/2016**") – hereinafter collectively referred to as Personal Data Protection Regulation ("**PDP Regulations**").

The "data privacy" concept was introduced in Indonesia through EIT Law, which is describing a privacy right as[1]: (i) the right to enjoy a private life and be free from all kinds of distractions; (ii) the right to be able to communicate with another person without being spied on; and (iii) the right to supervise information access regarding someone's personal life and data. The concept of "data privacy" has now been implemented through GR 71/2019 which replaces the previously prevailed Government Regulation No. 82 of 2012 on the Implementation of the Electronic System and Transaction. However, it must be noted that both regulations only cover data privacy in a general manner.

A more specific regulation on personal data protection is specified in 2016 through MCI Regulation 20/2016.. This regulation further addresses and regulates personal data protection within the Indonesian regulatory framework. A notable new provision to be mentioned is that GR 71/2019 has also introduced a standard definition of personal data which is normally used globally, in which personal data shall include any data on a person which is identified and/or may be identified individually or combined with other information both directly and indirectly through an Electronic System and non-electronic system.

The prevailing regulations covers the protection of personal data, including protection on collection, processing, analyzing, storage, display, reparation, update, announcement, delivery, dissemination and erasure of Personal Data conducted by Electronic System Operators ("**ESO**"). ESO is defined as any person, state administrator, business entity and community which provide, manage, and/or operate Electronic System, either individually or jointly, on towards Personal Data Subject for their own needs and/or the need of other parties. ESO shall include data controller and data processor. While there has yet to be a comprehensive provision on data controller/data processor under the prevailing laws, the government has started to put more responsibilities upon ESO in processing personal data. As the regulator, MCI is the relevant authority to enforce Data Protection issuances, while the State Cyber and Code Agency (locally known as "**BSSN**"), acts as the overseeing governmental body to consolidate and monitor all elements related to cyber security.

Aside from the above discussed, the Indonesian government has already drafted and submitted a draft bill on data protection ("**PDP Bill**") to the House of Representatives, in which approval is being deliberated. Enactment of the PDP Bill may effectively introduce new provisions similar to the EU General Data Protection Regulation ("**GDPR**"). Furthermore, there are also other sector specific legislations that govern data protection issues, among others, telecommunication, banking, financial services, and health provider services. Under such sectoral regulations, the relevant sectoral agency may become the supervisory body for data protection in the respective sectors.

Reference

[1] Elucidation of Article 26 paragraph (1) of EIT Law.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

Yes. In Indonesia, every ESO which is regulated or supervised by the MCI based on the provisions of laws and regulations; and/or ESO which has online portals, sites, or apps through the internet that are generally used in Indonesian territorial jurisdiction must conduct registration to MCI, as described below.

Mandatory Electronic System Registration ("ESO Registration")

Starting from 2019, every ESOs are now required to conduct electronic system registration with MCI. This requirement was previously directed to only ESOs whose business is related to provision of public services. However, prior to GR 71/2019, the regulation has incorporated criteria of public services broadly which can be stretched to almost any ESOs who conduct provision of goods or services to public. Rather than providing further clarification, the government now requires any ESOs, whether it is public or private ESO, to conduct mandatory electronic system registration with MCI.

In addition, MCI has just enacted a new implementing regulation on 24 November 2020 as the clearer provision on Offshore Private ESO in the midst of the growing online activity which involves electronic transaction and processing of personal data that particularly concerns private electronic system operator, MCI Regulation No. 5 of 2020 ("**MCI Regulation 5/2020**").

Prior to the enactment of MCI Regulation 5/2020, the implementation of ESO Registration by Offshore Private ESO was not a straightforward process and, subsequently, making such ESO Registration generally only applicable for onshore ESO, particularly due to the application documents for ESO Registration requiring local corporate documents.

MCI Regulation 5/2020 sets out new provisions on ESO Registration for Private ESO which is established not according to Indonesian law or permanently domiciled in another country but (a) providing services in the territory of Indonesia; (b) operating business activity in Indonesia; and (c) the Electronic System is being used and/or offered in the territory of Indonesia. Under this circumstance, an Offshore Private ESO needs to file a registration form addressed directly to MCI which contains several information among others:

- general description of the operation of Electronic System;
- its obligations on information security and personal data protection; and
- information on Offshore Private ESO including person in charge, domicile, number of customers, certificate of incorporation, or total transaction value originating from Indonesia.

Requirements in conducting registration is also elaborated in MCI Regulation No. 7 of 2018 regarding Electronic Integrated Licensing Service for Communication and Informatic Sector as lastly amended by MCI Regulation 7/2019 ("**MCI Regulation 7/2018**"). Under MCI Regulation 7/2018, in order to conduct registration, there are certain requirements which needs to be fulfilled e.g., general profile, corporate documents, tax identification number, and profile of company's contact person. In addition, ESOs who conduct registration must able to provide technical overview layout covering details on electronic system profile, URL website, domain name system / IP server address, brief description on Electronic System function and business process, explanation on utilization of hosting, and willingness to conduct personal data protection.

Appointment of Local Representative

Particularly in the case where a business is a foreign individual(s) or business entities incorporated and domiciled outside of Indonesia territory but actively conduct offering and/or trading through electronic system to consumers residing within Indonesia, our Governmental Regulation No. 80 of 2019 on Trade through Electronic Systems ("**GR 80/2019**") has put certain thresholds which may classify the abovementioned foreign businesses as physically present and operational as a permanent business establishment in Indonesia, as follows: (i) transaction volume; (ii) transaction value; (iii) volume of packages to be shipped; and/or (iv) volume of traffic or people who access the foreign Business Actor. Once the foreign businesses have fulfilled the certain thresholds, they will be required to appoint an Indonesia representative that will act on their behalf.

We understand that the above requirement is also related with government's purpose to tax overseas digital businesses. In fact, due to the Covid-19 pandemic, the government has decided to accelerate its plan to tax overseas digital businesses by enacting Government Regulation in Lieu of Law No. 1 of 2020 ("**PERPU 1/2020**"). Through this new regulation, the government may impose value added tax and income tax/electronic transaction tax to certain foreign e-commerce operators having a significant economic

presence in Indonesia which is considered as a permanent business establishment.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

Until to date, our PDP Regulations have not differentiated between personally identifiable information ("**PII**") from special or sensitive category PII. The broad definition of Personal Data under the PDP Regulations encompasses both PII and sensitive PII. However, the current draft of PDP Bill may establish a category of personal data to introduce differentiations which consist of a general and specific (deemed as sensitive category) category of personal data.

Please also be informed that depending on the sector of the business, there might be different type of data and treatment from the relevant authority in regards to how certain data is able to be collected and accessed by businesses. For instance, in the sector of (i) health – documents of medical record (data patients); (ii) financial company – data and information relating to consumer i.e., payment transaction, demographic data and information, and etc.; and (iii) peer to peer lending businesses (and its partners) – restricted to collect smartphone-based data from its users except for access to, among others, camera and IMEI.

4. What are the principles related to, the general processing of personal data or PII?

- **Lawful basis for processing personal data**

The key principle in general processing of Personal Data is to obtain consent from the relevant Data Subject. Unless provided otherwise by laws and regulations, use of any information through electronic media which involves Personal Data of a person must be made with the explicit consent from personal data subjects. Several exceptions where a consent may be waived is when certain Personal Data has been disclosed or published through the Electronic System for public services and when a lawful interception is exercised for law enforcement purposes.

- **Purpose limitation**

PDP Regulations stipulates that Personal Data may only be processed and analyzed in accordance with the specific purposes which have been expressly elaborated during the obtainment and collection of personal data. Therefore, in addition to obtaining approval from personal data through a consent form, it is necessary to ensure that the processing purposes are spelled out within such form and becomes a processing criterion.

- **Retention Period**

PDP Regulations sets out that the retention period of Personal Data shall be kept for at least 5 (five) years, starting from the last date the relevant Data Subject was considered a User. However, depending on the sectors concerned, the data retention period may differ.

- **Transparency**

There are two provisions in MCI Regulation 20/2016 that manifest in the transparency principle. Firstly, the Data Subject is entitled to get access or opportunity for obtaining history of Personal Data which is being transferred to ESO, to the extent in accordance with the prevailing laws and regulations. Secondly, the ESO is required to notify the Data Subject in the event of data breaches.

- **Internal Policy**

Data Controller is also required to have an internal policy in handling personal data as a prevention measures against any data breaches. The internal policy shall take into account technology implementation, human resources, methods, involved costs, and the prevailing laws and regulations.

- **Guaranteeing Data Privacy Rights**

As the owner of personal data, it is guaranteed with several basic rights in relation to the processing of its personal data by third party i.e., (i) right to data access; (ii) claims of damages; (iii) request of erasures / rights to be forgotten; and (iv) right to delisting (the right to request deletion of an electronic information in search engine).

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII and, if so, are there are rules relating to the form, content and administration of such consent?

As discussed above, consent is the key principle of Personal Data processing under the prevailing regulations in Indonesia. Consequently, consent from the Data Subject will always be required, except in certain events as stipulated in the prevailing laws and

regulations.

Furthermore, MCI Regulation 20/2016 requires that collection of consent shall be conducted by providing a consent form in Indonesian language which evidences the data subject's consent for the collection of his/her personal data by other third parties. However, the regulation is silent on specific formatting requirements of the consent form. It is sufficient provided that the purpose of processing Personal Data have been expressly stated during the collection of consent. For example, GR 71/2019 has stipulated several information which must be disclosed to the data subject, such as, identity of the ESO, protection of personal data guarantee, procedure for service utilization and security of electronic system.

6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

As discussed in Point 3 above, PDP Regulations does not recognize the concept of sensitive PII yet. In other word, there is no official categorization between PII and Sensitive PII and there is currently no differentiation between the data. Generally, any Personal Data can be obtained and processed as long as the ESO has explicitly already obtained the Data Subject's consent in accordance with the prevailing laws and regulations.

7. How do the laws in your jurisdiction address children's personal data or PII?

MCI Regulation 20/2016 stipulates that a minor or child are not able to provide consent for their own Personal Data. In the event that Data Subject is a minor, consent can only be provided by the parents or official guardian of the child. Note, if the concerned PII is above the age of 18, they then would be able to provide explicit consent in regards to such.

8. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

There is a safe harbor principle which may limit the liability of ESOs for any unlawful actions taken by its users specifically for certain type of ESO's service which enable a user generated content or enable parties to engage in any conduct within the ESO's electronic system. This was introduced under the newly enacted GR 80/2019 in order to provide certain protection to ESOs. Safe harbor would only be available provided that ESOs fulfill any of the following condition: (i) ESO is able to quickly delete any electronic link and/or illegal content following the discovery of such content, either by finding such content itself using its technology or through a report from public; or (ii) ESO can be classified as intermediary service operator who only provide intermediary/indirect services and only acting as mere conduit to support e-commerce activities, for example, search engine, hosting and caching provider.

9. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

Indonesian laws impose requirements of data protection both by design and by default. The data protection by design can be seen from the requirements imposed upon ESOs operating its electronic system in accordance with the personal data protection principles. Meanwhile, the data protection by default can be seen from the mandatory requirements to only obtain and gather information which are relevant and conforms with purposes specifically disclosed to the Data Subject during the collection of Personal Data.

In common practice, businesses are required to have sufficient technical and organizational policies/measures in place to implement the privacy and personal data protection principles. Furthermore, when collecting consent and data, the businesses will normally present privacy policy which clearly informs the Data Subject with the data processing and its specific purpose. Alongside with presenting privacy policy, businesses will provide a consent form in order to collect mandatory explicit consent from Data Subject. Businesses rarely process data unless Data Subject has provided its explicit consent.

10. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Pursuant to MCI Regulation 20/2016, ESO is required to provide audit trail for all Electronic System activities

which are managed by ESO, which includes collection and processing activities of Personal Data. On the other hand, Data Subject, as the owner of Personal Data, is not required to maintain any internal records. In practice, Data Subject will be granted sufficient control over the electronic system in order to exercise its rights of privacy and personal data protection.

11. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

In general, there is no mandatory obligation for ESO to conduct consultation with regulators regarding collection and processing of personal data. However, please be informed that in certain circumstances, such as (i) cross-border transfer of Personal Data; and (ii) data breach notification, ESOs is required to coordinate with the MCI or any relevant Supervisory Agency or Sectoral Regulator (if any). Please see our answer on point 20 regarding cross-border transfer from Indonesia to abroad and (ii) point 24 regarding data breaches notification to regulator.

12. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

Yes, GR 71/2019 requires ESO to implement risk management mechanisms against potential damage and loss that may result from threats, disturbance, and hinderance toward its electronic system. Such implementation of risk management shall be in the forms of risk analysis and formulation of mitigative and preventive steps against such incidents.

Please note however that stricter compliance may differ depending on the sector concerned.

13. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

Under the current prevailing regulations, there is no requirement to appoint a data protection officer or other designated person in respect of data protection. Under MCI Regulation 20/2016, ESO is only required to provide accessible contact person to the Data Subject in relation with processing of his/her Personal Data for the intent of contacting.

Please note however that data protection officer may be introduced in the PDP Bill.

14. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).

Under GR 71/2019, ESO is required to provide relevant information to Data Subject including privacy policy with relation to protection of personal data. Normally, the privacy notice is provided within the website and will be presented during the collection of consent and the beginning stage of data collection. This shall include any information on the purpose of collection, data processing activities and privacy/data protection guarantee.

Please note in the case that the specific use of data has changed, seeking of consent would then once again be required for the new use of data.

15. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (E.g. are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The prevailing regulation does not differentiate between Personal Data Controller and Personal Data Processor. Accordingly, any party that controls ("**Data Controller**") and processes ("**Data Processor**") any kind of electronic information, including Personal Data, in the form of electronic media, will be categorized as an ESO. Therefore, the current prevailing data protection regulation applies to the entire handling processes of Personal Data, starting from collection to processing of the same.

Nevertheless, in terms of any mandatory ESO's obligations and implementation of individual rights, the current prevailing regulation does not automatically stretch to Data Processor. It should be noted that the current PDP regulations tends to emphasizing its implementation to the relevant ESO that collects

personal data from relevant Data Subject (i.e., Data Controller). Therefore, any obligations of Data Processor shall be applied through contractual requirement from Data Controller. Furthermore, since Data Processor that acquires Personal Data from the Data Controller will only act on behalf of the latter, ESO collecting the Personal Data (i.e., Data Controller) is the one that possesses direct responsibility to the relevant Data Subject. In the event the Data Subject wishes to do certain actions or file requests against the Data Processor, it shall be made through the Data Controller.

16. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g. due diligence or privacy and security assessments)?

In general, there is no requirement of minimum contract terms, nor any forms of restriction, in respect of appointment of service providers under MCI Regulation 20/2016.

However, stricter compliance requirements shall apply for the use of information and technology in the banking sector, in which appointment of service provider shall involve a due diligence exercise and evaluation process. For instance, in regards to the appointment of service providers that provide information technology services, commercial banks will need to implement risk management among other requirements in order to be in compliance with the law.

17. Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

Indonesian laws do not recognize or acknowledge the terminology of 'cookies', but it may fall under the definition of Personal Data, given its broad definition. In such case, the general principle of 'consent' on Personal Data under Indonesian laws shall be applicable in the collection of cookies.

18. Please describe any laws in your jurisdiction addressing email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Until to date, only direct marketing via mobile network is being regulated. MCI Regulation No. 13 of 2019 regarding Telecommunication Services Provider ("**MCI Regulation 13/2019**") stipulates that Content Providers may offer content via a Network Operator, to the potential subscribers that have granted consent.

Email communication and direct marketing via online platforms are yet to be regulated under Indonesian legislations. However, GR 80/2019 does regulate electronic advertisement for marketing purposes in the form of text, sound, image and video which can be disseminated to the public through various electronic media facilities and/or electronic communication channels. Furthermore, although there are no specific provisions, through the general principle of consent, the relevant Data Subject may repudiate the consent over the use of his/her Personal Data for marketing purposes.

19. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

The prevailing regulations have yet to specifically address classification of Personal Data such as biometrics data, and therefore general principle of consent should be sufficient for collection and processing of biometrics. However, the concept is introduced and may be regulated as "specific data" in the PDP Bill. Under the PDP Bill, biometric data shall include individual physics, physiology and characteristic which are unique and identifiable, which shall include but are not limited to facial recognition, dactyloscopy data, eye retina and DNA sample.

20. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does cross-border transfer of personal data or PII require notification to or authorization form a regulator?)

Under MCI Regulation 20/2016 and GR 80/2019, there is no restriction of cross-border transfer of Personal Data in general, although there are certain compliance requirements that need to be fulfilled in order to achieve such, which are:

i. submission of notification regarding the intended transfer of Personal Data to abroad, which at least contains information of: the name of country of destination, the name of recipient, date of transfer, and purpose of transfer;
ii. requesting for advocacy, if required; and
iii. submission of report regarding the result of cross-border transfer.
iv. Personal data may be sent to another country or area outside Indonesia if the said country or area has been declared as having the same protection level and standard as Indonesia by the Minister.

Nevertheless, please be noted that the above applies to Personal Data in general, and a stricter regulation may apply depending on the sector, among others, financial and health sector.

Furthermore, specifically for ESO in the Public Sector, GR 71/2019 regulates that management, processing, and/or retention of the electronic system and data must be conducted within Indonesian territory, although the same regulation does provide exceptions and allows management, processing and/or retention of data outside Indonesia if the required retention technology is not available domestically.

21. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

In regard to security obligations, GR 71/2019 specifically requires ESO to implement several measures in order to protect their electronic system operational activity, including: (i) providing an audit trail for the purposes of monitoring, law enforcement, dispute settlement, verification, testing, incident response, and mitigation; (ii) securing the components of ESO's electronic systems; (iii) having and implementing procedure and facility for securing electronic systems to prevent and control system upon a threat and attack which causes a disturbance, failure, and loss; (iv) providing a security system including a system and procedure for handling and preventing any cyber threats; (v) preserving the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information maintained by ESO; and ensure that the Electronic System functions in accordance with its designation.

The above security obligations have also been elaborated in the MCI Regulation 20/2016 by requiring ESO that processes Personal Data to store all personal information in its possession in an encrypted form. Further, ESO is obliged to make internal regulations in respect of Personal Data protection as a form of preventive step to avoid breach protection. The internal regulations must consider several aspects i.e., technological applications, human resources, methods, costs and any other considerations which may be stipulated in other relevant laws and regulations. In addition, the preventive actions must at least comprise of the following activities: (i) raising the awareness of human resources within ESO's environment to provide Personal Data protection; and (ii) organizing training for the prevention of Personal Data protection failures in the electronic system under ESO's management.

22. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

The current prevailing law and regulations do not specifically address security breach. However, under EIT Law, there are several prohibited actions that may be considered as security breach, among others:

- Unlawful access to computers and/or Electronic Systems of other persons;
- Unlawful acquirement of electronic information and/or electronic records;
- Breaching, hacking into, trespassing into, or breaking through security of Electronic Systems;
- Unlawful alteration, addition, reduction, transmission, tampering with, deletion, moving, and/or hiding of electronic information and/or electronic records of other persons;
- Unlawful move or transfer of electronic information and/or electronic records to Electronic Systems of unauthorized persons; and
- Divulgence of confidential electronic information and/or electronic records to the public.

Based on the EIT Law, all of the abovementioned actions are subject to criminal sanctions in the forms of monetary penalty and/or imprisonment.

23. Does your jurisdiction impose specific security requirements on certain sectors or industries (e.g. telecoms, infrastructure)?

Yes. For Public Sector ESO (which would include certain infrastructure project), there are stricter personal data

compliance requirement that need to be met. Under MCI Regulation No. 4 of 2016 regarding Information Security Management System ("**MCI Regulation 4/2016**") for example, ESO for Public Services that utilizes strategic or high-level Electronic Systems must also employ SNI ISO/IEC 27001 as its standard information security management system.

Furthermore, as discussed above, there are also other sector specific legislations that govern data protection issues in the telecommunication, banking and financial services, and health provider services.

24. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

Reporting Obligation to Relevant Authority

Under the prevailing laws and regulations, ESO that suffers a serious data breach as a consequence of other parties' actions must immediately report to the relevant authority and Ministry at the first instance.

Further, ESO that suffers data breaches are required to notify the rightful owner of the data and may voluntarily file a complaint to Directorate General of Application Informatics of MCI ("**DGAI**") in the event of data breaches. This complaint shall be only intended as an effort to resolve any dispute amicably or other alternative dispute resolutions.

Reporting Obligation to Personal Data Subject

With regard to notice to the relevant Data Subject, ESO is obliged to provide notice for any incidences of data breaches to the Personal Data Subject ("**Notice of Breach**"). The Notice of Breach must at least contain the following information: (i) reasonings or causes of the data breaches occurrence; (ii) notice of breach can be submitted electronically provided that the relevant Personal Data Subject has approved such way of submission during the collection of his/her Personal Data; (iii) ensure that the relevant Data Subject has actually received the report if the incidence of data breaches may lead to potential loss; and (iv) a written report shall be submitted to the Personal Data Subject within 14 (fourteen) days after the data breaches came into realization.

25. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

Whilst the prevailing legal framework and guidance for cybersecurity in Indonesia is dispersed over a number of different regulations, the main reference for cybersecurity in Indonesia still refers to the EIT Law. However, the EIT Law regulates more so on the prohibition of cyber incidents (including, hacking, denial-of-service, phishing, identity theft) than describing the specific forms or guideline on cyber security measures that can be applied in Indonesia. Do note, in case of failure in protecting the managed Personal Data, the ESO must also notify such event as mentioned on point 24 above. Furthermore, in terms of cybercrime including intercepting or requesting information regarding electronic information of an individual, the law enforcement authority shall also possess the authority to obtain certain access to ESO's electronic system.

A notable mention that may affect the future of cybersecurity is that the government has previously submitted a draft bill on cybersecurity ("**Cybersecurity Bill**") which failed to pass the requirement to be enacted. However, to date, there is no clear timeline on the enactment of such draft bill in the future.

26. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

While the current regulation on cyber security is mostly being regulated under a governmental body and MCI's regulation as discussed above, the government has established a specific body called BSSN. We understand that BSSN is projected and tasked with responsibilities for any cyber security issues in Indonesia. BSSN's function includes the preparation, implementation, monitoring and evaluation of technical policies for the identification, detection, protection, control, regression, monitoring, evaluation, e-commerce protection control, encryption, filtering, cyber diplomacy, cyber crisis management center, cyber contact center, information center, mitigation and recovery support for cyber vulnerability, cyber incidents and/or cyber-attacks in Indonesia.

As per our understanding, the Cybersecurity Bill was supposed to provide BSSN with more power and authorities in implementing cyber security in Indonesia. However, since the bill failed to be enacted, the

regulation on cyber security is still mainly issued by BSSN and MCI, as the authority on communication and informatic sector. Therefore, depending on the development of the bill, there may possibly be a greater change of cybersecurity landscape in the future.

27. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

- **Access to Data**

As per one of an individual's right under MCI Regulation 20/2016, the Data Subject must have ease of access to his/her Personal Data for alteration, supplementation, and renewal purposes. This will also include the access on historical record of Personal Data transferred to the ESO. This individual's right is in line with one of the principles of Personal Data protection which is maintaining the integrity, accuracy, validity and up-to-dateness of Personal Data.

- **Right to Erasure**

Under Indonesian law and regulations, ESO is required to accommodate Data Subject's right to erasure of irrelevant electronic information including Personal Data. It is one of the rights of the Data Subject to request for deletion of certain information of his/her Personal Data. Such deletion shall entirely or partially remove documents pertaining to the Personal Data, either in the forms of electronic or non-electronic processing.

- **Right to Delisting**

GR 71/2019 introduces the right to delisting of irrelevant data from search engine listing. However, to do so, the Data Subject needs to petition such a request through the district court. In the events the court grants the petition to conduct delisting, the relevant court decision shall become the basis to request delisting of the irrelevant electronic information and/or document to the ESO.

28. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Under Indonesian laws, the individual rights are exercisable through both the judicial system and to a certain extent monitored and enforced by regulators. Further, in the event of ESO(s) failure in protecting personal data, in accordance with MCI Regulation 20/2016, the Data Subject can file a complaint to the MCI. The MCI may then form a personal data dispute resolution panel to pursue mutual resolution between the concerned Data Subject and ESO. If such mutual resolution is not reached, the Data Subject may then file a civil suit to exercises his/her individual rights in accordance with prevailing laws and regulations.

29. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

The individual rights are exercisable through the judicial system in the form of civil suit over breach of contract (i.e., breach of consent form or privacy policy) or tort. The same may also be exercised in the event of ESO's failure to protect Personal Data.

30. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Yes, the EIT Law accommodates the right of individual to file claim of monetary damages to the ESO by providing evidences of the actual damages suffered by the relevant Data Subject due to the transpired security breach.

31. How are the laws governing privacy and data protection enforced?

Enforcement of provisions within MCI Regulation 20/2016 is being conducted by the regulatory authority through direct or indirect supervision. It is also possible for the regulator to impose administrative sanctions in the forms of: (a) verbal warning; (b) written warning; (c) temporary suspension of activity; and/or (d) announcement on online websites. GR 71/2019 and GR 80/2019 also include additional administrative sanctions, such as access termination and license revocation.

Different institutions may also be involved and enforce data protection principle in other sectors including (i) Bank Indonesia as the authority in the banking sector, (ii) Financial Service Authority (or OJK) as the authority in the financial sector (including financial technology), and (iii) Ministry of Health as the authority in the medical sector. The administrative sanctions in these specific

sectors also varies accordingly. Criminal charges are also imposable on the violation of data privacy which is generally investigated by the police and prosecuted by the state prosecutor.

32. What is the range of fines and penalties for violation of these laws?

Aside from administrative sanctions, EIT law provides criminal sanctions in the form of jail sentences up to 10 years and/or fines up to 5 billion rupiah, imposable to any subject who unlawfully alters, adds, reduces, transmits, tampers with, deletes, moves, hides electronic information and/or electronic documents of other persons or of the public to electronic systems of unauthorized persons or when such action results in them being compromised such that the data becomes accessible to the public in its entirety in an improper manner.

While the prevailing MCI Regulation 20/2016 does not provide any criminal sanctions, the latest deliberated PDP Bill planned for 2021 details some criminal sanction articles imposable on data privacy offenders.

33. Can personal data or PII owners/controller appeal to the courts against orders of the regulators?

Yes. ESO imposed with administrative sanctions may appeal the sanctions given in the form of decree, which is normally awarded for the suspension, to the Indonesian State Administrative Court.

Contributors

Enrico Iskandar
Founding Partner
enrico@bepartners.co.id

Bratara Damanik
Principal Associate
bratara@bepartners.co.id

Alwin Widyanto Hartanto
Associate
alwin@bepartners.co.id