The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Indonesia: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection and cyber security laws and regulations that may occur in Indonesia.

This Q&A is part of the global guide to Data Protection & Cyber Security. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/practice-areas/data-protection-cyber-security/

Country Author: Bagus Enrico & Partners (BE Partners)

The Legal 500

Enrico Iskandar, Partner

enrico@bepartners.co.id

The Legal 500

Bimo Harimahesa, Senior Associate

bimo@bepartners.co.id

Bratara Damanik, Associate

bratara@bepartners.co.id

1. **Please provide an overview of the legal 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 laws enforced)?**

The “data privacy” concept is firstly introduced through two main legislations, namely: (i) Law No 11 of 2008 on Electronic Information and Transaction, lastly amended by Law No. 19 of 2016 (“ ***EIT Law*** ”); and (ii) Government Regulation No. 82 of 2012 on the Implementation of the Electronic System and Transaction (“GR 82/2012”). However, these two aforesaid laws only cover data privacy in general manner.

In 2016, as the implementing regulation of EIT Law and GR 82/2012, Ministry of Communication and Informatics (“***MCI***”) issued its Regulation No. 20 of 2016 regarding Personal Data Protection in the Electronic System (“***MCI Regulation 20/2016***”) to further regulate personal data protection issue in Indonesian regulatory framework. In general, MCI Regulation 20/2016 covers the protection of personal data, including protection on collection, processing, analyzing, storage, display, announcement, delivery, dissemination and erasure of Personal Data conducted by Electronic System Operator (“***ESO***”). As the regulator, MCI is the relevant authority to enforce MCI Regulation 20/2016.

Under MCI regulation 20/2016, Personal Data is defined as certain individual information that are kept and maintained, and its accuracy and confidentiality is protected. Based on the given definition, all individual information collected and processed by ESO are protected under MCI Regulation 20/2016.

Meanwhile, MCI Regulation 20/2016 defines ESO 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. Based on the above definition, Indonesia regulation does not define or 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 ESO.

Aside from MCI Regulation 20/2016, there are other sector specific legislations that govern data protection issue, among others, banking, financial services, and health provider services. Under these sectoral regulations, the relevant sectoral agency may become the supervisory body for data protection in the respective sectors.

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?**

Depending on the category of ESO that processes Personal Data, a registration may be required. Based on GR 82/2012, ESOs are divided into two categories i.e., (i) ESO for Public Services, and (ii) ESO for Non-Public Services. Under the same regulation, ESOs for Public Services are required to conduct a registration while ESO for Non-Public Services may choose to register on a voluntary basis. Therefore, the registration is only mandatory to ESO for Public Services.

The further definition of ESO for Public Services is stipulated within MCI Regulation No. 36 of 2014 regarding Electronic System Operator ("**MCI Regulation 36/2014**"). Under MCI Regulation 36/2014, ESO for Public Services includes state-institutions, state-owned enterprises, and other legal entities that conduct public services for the purpose of state mission implementation. Specifically, the said legal entity refers to ESO that owns:

(a) A web portal, website, or online application via the internet that is used to facilitate offering and/or trading of goods and/or services.

(b) An electronic system that contains a payment facility and/or other financial transaction facilities online by means of communication of data or via the internet.

(c) An electronic system used to process electronic information which contains or requires deposit of funds or other similar form of funds.

(d) An electronic system used to process, administer, or store data related to facilities that are associated with customer data for public serving operational activity on financial transactions and trading activity.

(e) An electronic system used for the delivery of payable digital material through a

data network, either by means of download via web portal/website, email transmission, or other application to the user device.

Requirements in conducting registration is further elaborated in MCI Regulation No. 7 of 2018 regarding Electronic Integrated Licensing Service for Communication and Informatic Sector ("***MCI Regulation 7/2018***"). Under MCI Regulation 7/2018, in order to conduct registration, there are certain requirements which need to be fulfilled including general profile, corporate documents, tax identification number, profile of company's contact person, and certification of information security based on Electronic System category. In addition, ESO 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.

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

The current prevailing regulations have not differentiated between personally identifiable information ("**PII**") and sensitive PII. The broad definition of Personal Data under MCI Regulation 20/2016 covers both PII and Sensitive PII.

4. **Are there any restrictions on, or principles related to, the general processing of PII – for example, must a covered entity establish a legal basis for processing PII in your jurisdiction or must PII only be kept for a certain period? Please outline any such restrictions or "fair information practice principles" in detail?**

MCI Regulation 20/2016 adopts several principles related to the general processing of

Personal Data:

- Lawful basis for processing
  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 approval of the relevant person. 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
  It is important that the purpose of processing Personal Data is in accordance and have been expressly stated during the collection of Personal Data. Under MCI Regulation 20/2016, ESO is not allowed to carry out any personal data process which is not within the scope of processing purposes spelled out within the Data Subject's consent form.
- Data minimisation

  MCI Regulation 20/2016 regulates ESO to only obtain and gather information which are relevant and conform with purposes disclosed to the Data Subject during the collection of Personal Data. Determination of such relevant information may be decided by a Supervisory Agency or Sectoral Regulator.

- Retention Period

  With regard to the Personal Data retention period, MCI Regulation 20/2016 refers to laws and regulations as set out by the relevant Supervisory Agency and Sectoral Regulator. However, should there be no statutory that specifically govern it, MCI Regulation 20/2016 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.

- 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.

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

As discussed above, the general principle of consent is the key principle of Personal Data processing under MCI Regulation 20/2016. Consequently, consent from the Data Subject will always be required, except in certain events as stipulated in the laws and regulations.

With regard to the consent form, MCI Regulation 20/2016 requires ESO to provide a consent form with Indonesian language in obtaining approval from the relevant Data Subject. However, the regulation is silent on the formatting requirements of the consent form.

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

As discussed in Point 3 above, MCI Regulation 20/2016 does not distinguish between PII and Sensitive PII. Generally, any Personal Data can be obtained and processed as long as the ESO 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 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.

8. **Are owners or processors of 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 only required to provide audit trail for all Electronic System activities which 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.

9. **Are consultations with regulators recommended or required in your jurisdiction and in what circumstances?**

   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 cross-border transfer of Personal Data from Indonesia to abroad, ESO is required to coordinate with MCI or any relevant Supervisory Agency or Sectoral Regulator (if any). Please see our answer on point 15 regarding cross-border transfer.

10. **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?**

    There is not any specific requirement to conduct risk assessments regarding data processing activities. However, GR 82/2012 requires ESO to implement risk management against potential damage and loss that may result from threat,

disturbance, and hinderance toward its electronic system. It is further elucidated that the implementation of risk management shall be in the forms of risk analysis and formulation of mitigative and preventive steps against such incidents.

11. **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? What are the data protection officer's 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.

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

Under Indonesian laws, there are no explicit requirements to provide privacy notice to the Data Subject. However, MCI Regulation 20/2016 does require ESO to obtain consent on how it processes and analyzes the Personal Data during the data collection. Normally, explanation of the processing activities will be included within the Consent Form provided to the Data Subject.

13. **Do the laws in your jurisdiction apply directly to service providers that process PII, or do they typically only apply through flow-down contractual requirements from the owners?**

Ideally, MCI Regulation 20/2016 applies to the entire handling processes of Personal Data, starting from collection to processing of the same. Consequently, any ESO that take up any of the handling process of Personal Data should also be bound to MCI Regulation 20/2016.

Nevertheless, in terms of implementation of individual rights, we are of the view that MCI Regulation 20/2016 does not automatically stretch to the Data Processor. 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. Therefore, 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.

14. **Do the laws in your jurisdiction require minimum contract terms with service providers or are there any other restrictions relating to the appointment of service providers (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 banking sector, in which appointment of service provider shall involve a due diligence exercise and evaluation process.

15. **Is the transfer of PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (for example, does cross-border transfer of PII**

require notification to or authorization form a regulator?)

Under MCI Regulation 20/2016, there is no restriction of cross-border transfer of Personal Data, but there are certain compliance requirements that need to be fulfilled, 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.

Nevertheless, there is lack of supervision from the MCI in the implementation of the above compliance requirements.

Specifically, for ESO for Public Services, GR 82/2012 requires them to place their data center within the territory of the Republic Indonesia. By this provision, ESO for Public Services that manages Personal Data may be prohibited from transferring the Personal Data to any party located in other countries for storing purposes. In practice, it is common for private business entities that are considered as ESO for Public Services to outmaneuver this requirement by taking up practical approach on the arrangement of storages location.

16. **What security obligations are imposed on PII owners and on service providers, if any, in your jurisdiction?**

In regard to security obligations, GR 82/2012 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 avoid disruption, failure, and loss; (iv) providing a security system including a system and procedure for handling and preventing any cyber threats; and (v) preserving the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information maintained by ESO.

The above security obligations have been further 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.

Further, there are stringent requirement for ESO for Public Services in respect of security obligation. Under MCI Regulation No. 4 of 2016 regarding Information Security Management System ("**MCI Regulation 4/2016**"), the ESO for Public Services is divided into three categories based on their risks, namely: (i) strategic electronic systems, which have a serious impact on public interest, public services, state administration continuity, or national security and defense; (ii) high-level electronic systems, which have limited impact for sectoral and/or regional interests; and (iii) low-level electronic systems, which do not fall under the categories of strategic and high-level electronic systems. Specifically, for ESO for Public Services who utilizes strategic or high-level Electronic Systems must employ SNI ISO/IEC 27001 as its standard information security management system.

17. Does your jurisdiction impose requirements of data protection by design or default?

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 to ESO in 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 conform with purposes specifically disclosed to the Data Subject during the collection of Personal Data.

18. **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 unauthorised persons; and
- Divulgence of confidential electronic information and/or electronic records to the public.

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

19. **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 law and regulation, ESO is not legally required to conduct report of system breach over data protection to the MCI. ESO that suffers data breaches 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.

20. **Do the laws in your jurisdiction provide individual rights, such as the right to access and the right to deletion? If so, please provide a general description on what are the rights, how are they communicated, what exceptions exist and any other relevant details.**

- ***Access to Data***
  As one of the 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 Deletion***
  Under Indonesian law and regulations, ESO is required to provide a deletion mechanism 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.

21. **Are individual rights exercisable through the judicial system or enforced by a regulator or both? When exercisable through the judicial system, does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances? Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury of feelings sufficient?**

Under Indonesian laws, the individual rights are exercisable through the judicial system in the form of civil suit over breach of contract (e.g., consent form or privacy policy) or tort. 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.

22. **How are the laws governing privacy and data protection enforced? What is the range of fines and penalties for violation of these laws? Can PII owners appeal to the courts against orders of the regulators?**

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

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

Aside from the above, MCI Regulation 20/2016 also mandates that ESO must acquire certification of its electronic system in order to conduct collection and processing of Personal Data, which is supposed to be further regulated in an implementing regulation. However, until to date, there has been no regulation issued to govern such certification requirement.

24. **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.

25. **Please describe any laws addressing email communication or direct marketing?**

Until to date, only direct marketing via mobile network is being regulated. MCI Regulation No. 9 of 2017 regarding Content Providing Services Operation on Cellular Mobile Network ("***MCI Regulation 9/2017***") stipulates that Content Providers may only offer content via a Network Operator, to the potential subscribers that have granted opt-in consent. In the event there are users who have expressed their objection or rejection, the Network Operators are prohibited to transmit such content.

Email communication and direct marketing via online platforms are yet to be regulated

under Indonesian legislations. Although there is no specific provision, 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.