Indonesia


Enrico Iskandar


Bimo Harimahesa

Bagus Enrico & Partners

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Ministry of Communications and Informatics (*Kementerian Komunikasi dan Informatika*/"**MCI**") recently promulgated the principal data protection legislation in Indonesia, namely MCI Regulation No. 20 of 2016 regarding Personal Data Protection in the Electronic System ("**MCI Regulation 20/2016**").

1.2 Is there any other general legislation that impacts data protection?

MCI Regulation 20/2016 serves as the implementing regulation of the following general laws: (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**").

Prior to the enactment of MCI Regulation 20/2016, EIT Law and GR 82/2012 introduced the 'data privacy' concept and became the primary source of provisions on data protection.

1.3 Is there any sector specific legislation that impacts data protection?

There are specific pieces of legislation in various sectors which impact data protection which, among others, are:

(i) Government Regulation No. 96 of 2012 on the Implementation of Public Services.

(ii) Bank Indonesia's Regulation No. 9/15/PBI/2007 on the Implementation of Risk Management in the Utilisation of Information Technology by the Bank.

(iii) Decree of Head of SKK Migas PTK-008/SKO0000/2013/S0 on the Information and Telecommunication Technology Management over Production Sharing Contract Contractors.

(iv) Government Regulation No.46 of 2014 on Health Information System.

(v) Financial Services Authority Regulation No. 77/POJK.01/2016 on the Information Technology-Based Money Lending Services.

(vi) MCI Regulation No. 36 of 2014 on the Registration Procedure of Electronic System Operator ("**MCI Regulation 36/2014**").

(vii) MCI Regulation No. 4 of 2016 on the Information Security Management System ("**MCI Regulation 4/2016**").

(viii) MCI Regulation No. 9 of 2017 on Content Providing Services Operation on Celullar Mobile Network ("**MCI Regulation 9/2017**").

1.4 What is the relevant data protection regulatory authority(ies)?

Pursuant to MCI Regulation 20/2016, the authority responsible for supervising data protection activity is the Minister of Communications and Informatics and/or Head of Supervisory Agency and Sectoral Regulator.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"

  Both GR 82/2012 and MCI Regulation 20/2016 share the same definition of "Personal Data", which is certain individual information that are kept and maintained, and its accuracy and confidentiality is protected. However, GR 82/2012 does not provide further explanation on what information qualifies as "Personal Data".

- "**Sensitive Personal Data**"

  Currently, there are no definitions provided under MCI Regulation 20/2016, GR 82/2012, nor EIT Law with regard to "Sensitive Personal Data".

- "**Processing**"

  MCI Regulation 20/2016 does not specifically define "Processing". However, MCI Regulation 20/2016 described that protection of Personal Data in Electronic System shall be conducted in the following processes: (i) acquiring and collection; (ii) processing and analysis; (iii) retention; (iv) exhibition, announcement, transfer, dissemination, and/or open access; and (v) deletion.

- "**Data Controller**"

  MCI Regulation 20/2016, GR 82/2012, nor EIT Law specifically define "Data Controller", but please see the definition of Electronic System Operator below.

- "**Data Processor**"

  MCI Regulation 20/2016, GR 82/2012, nor EIT Law specifically define "Data Processor", but please see the definition of Electronic System Operator below.

- "**Data Subject**"

  MCI Regulation 20/2016 uses the term of "Personal Data Owner", which means individual to whom Certain Individual Data is attached.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  "**Electronic System**"

  "Electronic System" means a set of electronic equipment and procedures that are used to prepare, collect, process, analyse, store, display, publish, deliver, and/or distribute electronic information.

  - "**Electronic System Operator**"

    "Electronic System Operator" (*Penyelenggara Sistem Elektronik*/"**ESO**") means any person, state administrator, business entity, and public that provides, manages, and/or operates an Electronic System, either individually or jointly, to the Electronic System users for the interests of its own and/or other parties.

    By this definition, ESO shall mean the party that controls and processes any kind of electronic information, which includes Personal Data in the form of electronic media.

  - "**Electronic System User" or "User**"

    "Eletronic System User" means any person, state administrator, business entity, and public that utilises goods, services, facility or information provided by the ESO.

  - "**Public Services**"

    "Public Services" means an activity or series of activities in order to fulfil service needs in accordance with the prevailing laws and regulations for every citizen and resident upon goods, services, and/or administrative services provided by a Public Services Provider.

  - "**Public Services Provider**"

    "Public Services Provider" means any institution of state administrators, corporations, independent institutions established under laws for public services purposes, and other legal entities formed solely for public services purposes.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  There are two provisions in MCI Regulation 20/2016 that manifest in the transparency principle.

  Firstly, the Personal Data Owner 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 Personal Data Owner in the event of data breaches. See question 13.3 below.

- **Lawful basis for processing**

  The key principle in establishing lawful basis for processing Personal Data is to obtain the Personal Data Owner's consent. Unless provided otherwise by laws and regulations, use of any information through electronic media that involves Personal Data of a person must be made with the approval of the relevant person.

  Further, MCI Regulation 20/2016 requires ESO to provide a consent form with Indonesian language in obtaining approval from the relevant Personal Data Owner. In addition, MCI Regulation 20/2016 also stipulates Personal Data which may be processed and analysed is Personal Data in which its accuracy has been verified.

  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**

  MCI Regulation 20/2016 stipulates that Personal Data may only be processed and analysed in accordance with ESO's needs that have been expressly stated during the obtainment and collection of Personal Data. Related to the requirement of obtaining approval from the Personal Data Owner through a consent form, it is necessary to ensure that the processing purposes are spelled out within such form and become processing criterion for the ESO.

- **Data minimisation**

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

- **Proportionality**

  EIT Law, GR 82/2012 and MCI Regulation 20/2016 do not have any provision on proportionality.

- **Retention**

  MCI Regulation 20/2016 refers to laws and regulations as set out by the relevant Supervisory Agency and Sectoral Regulator with regard to the Personal Data retention period. 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. By the time a Personal Data Owner is no longer considered as a User, ESO is obliged to store the relevant Personal Data starting from the last date the Personal Data Owner was considered a User.

  Moreover, see the requirement of data centre location in question 11.1 below and encryption obligation in question 13.1 below.

- *Other key principles – please specify*

  - **Right to be Forgotten**

    The latest amendment of EIT Law adopts the principle of Right to be Forgotten. EIT Law stipulates that every ESO has the obligation to delete irrelevant Electronic Information and/or Electronic Document under its possession upon request of the related person by virtue of a court order. Every ESO must also provide a deletion mechanism of irrelevant Electronic Information and/or Electronic Document in accordance with the prevailing laws and regulations. EIT Law sets out that the foregoing deletion procedure will be further stipulated in a Government Regulation, which has not been issued until the date of this report.

  - **Electronic System worthiness**

    The Electronic System used for processes involved in the protection of Personal Data must undergo a certification procedure. The procedure of certification shall be made in accordance with the prevailing laws and regulations. Under MCI Regulation 4/2016, certification is only mandatory for Electronic Systems that are categorised strategic or high-level. An Electronic System is considered strategic when it has serious impact to public interests, Public Services, continuity of State operational activity, or State defence and security. Furthermore, an Electronic System is considered high-level when it has limited impact on the interest of certain sectors and/or regions.

MCI Regulation 20/2016 also requires an Electronic System that is used to facilitate the acquiring and collection of Personal Data to use official software and to posses qualifications of interoperatibility and compatibility. By this, interoperatibility means the ability of the different Electronic Systems to operate in an integrated manner, whilst compatibility means conformity of one Electronic System with another.

- **Internal policy**

  MCI Regulation 20/2016 requires ESO to have an internal policy in processing the Personal Data as a prevention measure against data breaches. The internal policy shall take into account technology implementation, human resources, methods, involved costs, and the prevailing laws and regulations. Other prevention measures that must be conducted by the ESO are among others increasing awareness of human resources in its environment to provide Personal Data protection in the Electronic System managed by them; and organising training to the human resources on the subject of data breaches prevention.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  It is one of the principles of Personal Data protection under MCI Regulation 20/2016 that the integrity, accuracy, validity and up-to-dateness of Personal Data must be maintained by ESO. Accordingly, Personal Data Owner must have ease of access to his/her Personal Data for alteration, supplementation, and renewal purposes. Additionally, Personal Data Owner is also entitled to gain access on historical record of Personal Data transfer to ESO.

- **Correction and deletion**

  It is the rights of the Personal Data Owner that any corrections made by him/her to the Personal Data shall not interrupt the management system of the same, unless stipulated otherwise by the prevailing laws and regulations.

  Meanwhile, deletion of Personal Data may only be carried out if the retention period stipulated under MCI Regulation 20/2016 has lapsed or based on a request from the Personal Data Owner. Such deletion shall entirely or partially remove documents pertaining to the Personal Data, either in the forms of electronic or non-electronic processing, managed by ESO and/or User so that the said Personal Data could no longer be displayed in the Electronic System save for being provided with new Personal Data by the Personal Data Owner.

- **Objection to processing**

  Through the mechanism of 'consent', the Personal Data Owner may repudiate the consent over processing of his Personal Data.

- **Objection to marketing**

  Through the mechanism of 'consent', the Personal Data Owner may repudiate the consent over the use of his Personal Data for marketing purposes.

- **Complaint to relevant data protection authority(ies)**

  Every Personal Data Owner and ESO may file a complaint to the Directorate General of Application Informatics of MCI ("**DGAI**") in the event of data breaches, but such complaint is only intended as an effort to resolve the dispute amicably or through other alternative dispute resolutions. Following such claim, the DGAI may then coordinate with heads of Supervisory Agency or Sectoral Regulator or form a Personal Data dispute settlement panel.

- *Other key rights – please specify*

  - **Determination of confidential and non-confidential Personal Data**

    The Personal Data Owner shall be granted with options to determine the confidentiality and non-confidentiality of his/her Personal Data. Nonetheless, such options will not be applicable if the prevailing laws and regulations excplicitly state that some elements of a particular Personal Data are determined confidential in nature.

  - **Claims of damages**

    EIT Law stipulates that any person whose rights are infringed on the subject of Personal Data may submit a claim for damages incurred. Such claim may be submitted by filing a civil suit to the Indonesian district court.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

Subject to ESO's general category that processes Personal Data, a registration may be necessary. Under GR 82/2012, ESO is divided into two categories, which are (i) ESO for Public Services, and (ii) ESO for Non-Public Services. ESO for Public Services are required to conduct a registration; meanwhile, any ESO for Non-Public Services may choose to register on a voluntary basis.

International transfer of Personal Data specifically requires a notification to the authority. See question 8.3 below.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

The registration shall be made per legal entity, meaning by each of the ESO.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

MCI Regulation 36/2014, which is the implementing regulation of GR 82/2012 on the subject of ESO registration requirement, provides further definition of ESO for public services. Other than covering state institutions/agencies and state-owned enterprises, the definition of ESO for public services under MCI Regulation 36/2014 also covers other legal entities which conduct public services for the purpose of state mission implementation. In particular, the said legal entity refers to ESO that owns:

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 data or via the internet.

c. An Electronic System used to process electronic information which contains or requires deposit of funds or other similar forms 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 transaction and trading activity.

e. An Electronic System used for the delivery of payable digital material through a data network, either by means of a download via web portal/website, email transmission, or other application to the user device.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

Other than the general profile, licences, and corporate documents of the relevant ESO, in particular, the registration shall include the Electronic System technical overview layout which covers details on software, hardware, expertise workforce, management system, scope of public services, and interoperability with other electronic systems (if relevant).

5.5 What are the sanctions for failure to register/notify where required?

MCI Regulation 36/2014 does not stipulate any sanction on failure to comply with the ESO registration requirement.

5.6 What is the fee per registration (if applicable)?

There is no applicable fee for the ESO registration.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

Upon being registered, the ESO shall be granted with a Registration Certificate which is valid for a period of 5 (five) years. Renewal of the Registration Certificate will be valid for another period of 5 (five) years, which shall be submitted at the latest 5 (five) days before the expiration of the preceding Registration Certificate.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

There is no provision under EIT Law, GR 82/2012, or MCI Regulation 20/2016 to obtain prior approval for particular types of processing activities of Personal Data from the MCI. Even the requirement of notification for international data transfer does not involve approval request submission to the MCI.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

See question 5.8 above.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

There are no requirements for the appointment of a Data Protection Officer under EIT Law, GR 82/2012, or MCI Regulation 20/2016.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

See question 6.1 above.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

See question 6.1 above.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

See question 6.1 above.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

See question 6.1 above.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

See question 6.1 above.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

There are no legislative restrictions on the sending of marketing communications under Indonesian laws. The general principle of 'consent' shall also apply in marketing communications.

On a side note, MCI Regulation 9/2017 stipulates that Content Providers may only offer Contents, via a Network Operator, to the potential subscribers that have granted opt-in consent. Network Operators, however, are prohibited to transmit the offers to network users who have expressed their objection or rejection. It is also provided that the offers of Contents shall not charge any delivery fees to the network users as the recipient.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

MCI is considered inactive with regard to enforcement of breaches of marketing restrictions. MCI Regulation 9/2017 honours the protection of users against any privacy intrusion and disturbing offers, but mandating the protection measures to the Content Providers and Network Operators.

7.3 Are companies required to screen against any "do not contact" list or registry?

There is no specific regulation under Indonesian laws regarding a do-not-contact list or registry.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

There are no specific penalties which can be imposed upon breach of marketing communications restrictions.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

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

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

See question 7.5 above.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

See question 7.5 above.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

See question 7.5 above.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad.

In general, there is no prohibition to transfer Personal Data abroad, but MCI Regulation 20/2016 requires the ESO to coordinate with MCI or, if applicable, the relevant Supervisory Agency or Sectoral Regulator. Certainly, consent from the Personal Data Owner must be firstly obtained prior to the proposed transfer of Personal Data abroad.

It should be noted, however, that GR 82/2012 sets out a requirement to ESO for Public Services to place their data centre within the territory of the Republic of Indonesia. By this provision, ESO for Public Services that manages Personal Data may be prohibited from transferring the Personal Data which it manages to any party located in other countries for storing purposes (e.g., cloud services). See question 11.1 below for further details.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

There is no general mechanism to transfer Personal Data abroad under Indonesian laws.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

As explained, the transfer of Personal Data to outside the territory of the Republic of Indonesia must be coordinated with the MCI or relevant Supervisory Agency or Sectoral Regulator, but does not require approval. The coordination required by MCI Regulation 20/2016 shall involve the following: (i) notification of the intended transfer of Personal Data abroad, which at least contains the name of the recipient country, full name of the recipient subject, date of transfer and reasonings/purposes of transfer; (ii) seeking advocacy, if needed; and (iii) reporting of the Personal Data transfer implementation result.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

Corporate whistle-blowers are not regulated under Indonesian laws. Nevertheless, the whistle-blowing system has been implemented in several agencies in Indonesia, such as the Ministry of Finance, the Ministry of Energy and Mineral Resources, and Financial Services Authority, as well as in several major public-listed companies in Indonesia. Respectively, these agencies and companies have their own whistle-blowing system guidelines and policy.

Reporting of issues must be related to the relevant agency/company and the alleged violation must be conducted by the employee/officer of the said agency/company. Mostly, the person who submits the report must also be the employee/officer of the relevant agency/company.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

There is no applicable law or binding guidance issued by the MCI and it may be subject to the policy of each of the companies. In some companies, however, the whistle-blower is given with an option to submit the report anonymously.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

No, since corporate whistle-blowers are not being regulated in Indonesian laws.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

No, since corporate whistle-blowers are not being regulated in Indonesian laws.

9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There is no regulatory requirement to notify or consult the works councils/trade unions/employee representatives for the use of CCTV and employee monitoring. This will be subject to the Company Handbook or Collective Labor Agreement of the relevant company.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?

No, the use of CCTV is not being distinguished with the general acquiring and collection of Personal Data under MCI Regulation 20/2016.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Indonesian laws do not regulate employee monitoring.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Although not being regulated under Indonesian laws, CCTV and employee monitoring shall be considered as a general acquiring and collection of Personal Data; therefore, the general principle of 'consent' shall also apply in this case. The consent from the employee for the use of CCTV and employee monitoring may be obtained in the employment contract or the company regulation/ collective labour agreement.

10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There is no regulatory requirement to notify or consult the works councils/trade unions/employee representatives for the use of CCTV and employee monitoring. This will be subject to the Company Handbook or Collective Labor Agreement of the relevant company.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, see question 10.3 above.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Both GR 82/2012 and MCI Regulation 20/2016 expressly restrict ESO for Public Services to place its data centre overseas. Therefore, in the event that the ESO for Public Services would like to engage in cloud-based storing services, the cloud server must be located within the territory of the Republic of Indonesia.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There isn't any general specific contractual obligations required by the MCI to be entered by ESO with a cloud-based services provider. Nevertheless, requirement of a specific contractual obligations may be applicable on a sectoral level, such as in the banking sector.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

IT Law, GR82/2012, and MCI Regulation 20/2016 do not regulate the utilisation of big data and analytics.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

MCI Regulation 20/2016 requires ESO to store all Personal Data in its possession in an encrypted form. However, there is no further stipulation on the encryption mechanism to be implemented by the ESO.

In addition, under MCI Regulation 4/2016, ESO for Public Services that utilises strategic or high-level Electronic Systems must employ SNI ISO/IEC 27001 as its standard information safety management system.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

There is no legal requirement to report breach over data protection to the MCI. As described in question 4.1 above, the Personal Data Owner or ESO that suffers data breaches may voluntarily file a complaint to the DGAI as an effort to resolve the dispute.

Filing of the complaint must be made within 30 (thirty) days after the claimant realised the occurrence of data breaches. The complaint shall be submitted in writing containing: (i) claimant name and address; (ii) complaint grounds/reasonings, (iii) request of settlement of the submitted dispute; and (iv) place and time of complaint submission along with the claimant's signature. Filing of the complaint must also be supplemented with supporting evidences.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

MCI Regulation 20/2016 requires ESO to report any incidence of data breaches to the Personal Data Owner with the following terms: (i) the report must include reasonings or causes of the data breaches occurrence; (ii) the report may be submitted electronically provided that the relevant Personal Data Owner has approved such way of submission during the collection of his/her Personal Data; (iii) ensure that the Personal Data Owner 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 Owner within 14 (fourteen) days after the data breaches came into realisation.

13.4 What are the maximum penalties for security breaches?

EIT Law imposes penalties only over criminal acts in the IT sector and against the party who conducts the security breaches, not to ESO which handles the Personal Data.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/administrative Sanction	Criminal Sanction
Request of data and information from ESO for data protection purposes that may be conducted periodically or at any time.	Any persons that obtain, collect, process, analyse, store, display, publish, deliver, and/or distribute Personal Data not in accordance with MCI Regulation 20/2016 or other prevailing laws and regulations may be imposed with the following administrative sanctions: (a) verbal warning; (b) written warning; (c) temporary suspension of activity; and/or (d) announcement on online websites.	This is not applicable.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Under EIT Law, the MCI is granted with the authorities to receive reports or complaints on any criminal acts in the IT sector, summoning witnesses, performing investigation towards suspected parties and the relevant IT equipment and/or devices, conducting a search within the suspected crime scene, confiscating IT equipment and/or devices, and requesting expert assistance.

Due to the recent issuance of MCI Regulation 20/2016, we are not aware of recent cases on the implementation of the MCI's powers to impose the administrative sanctions described in question 14.1.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is currently no specific provision regarding a companies' response towards foreign e-discovery or disclosure requests from foreign law enforcement agencies. However, EIT Law stipulates that in order to resolve criminal actions, Indonesian investigators may cooperate with foreign investigators through exchanging information and evidences.

15.2 What guidance has the data protection authority(ies) issued?

There is currently no official guide issued by the MCI with regard to the exchange of information and evidences between Indonesian investigators and foreign investigators.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

In September 2016, the Indonesian Constitutional Court has granted a request of judicial review submitted by the suspected perpetrators of a corruption act, which led to the amendment of EIT Law by virtue of Law No. 19 of 2016.

The judicial review is based on questionable legal evidence submitted during the trial proceedings of the perpetrator, which is an unlawful recording of a conversation involving the suspect. Since lawful interception for law enforcement purposes must be based on an official request issued by the relevant authorities, an unlawful recording of a conversation shall be deemed as a breach of Personal Data protection. Although debatable and what might be politically influenced, this case law shows how protection of Personal Data may even outweigh the criminal investigation process under the Indonesian judiciary system.

16.2 What "hot topics" are currently a focus for the data protection regulator?

The MCI Regulation 20/2016 provides a 2 (two) years adjustment period for ESO(s) that have been managing Personal Data prior to the issuance of the said regulation. Due to the ongoing adjustment period, the MCI is currently still focusing on the promotion of Personal Data protection by ways of socialisation, technical guidance,advocacy, and other means of media.

Enrico Iskandar
Bagus Enrico & Partners
DBS Bank Tower, 17th floor, Suite 1701
Jl. Prof. Dr. Satrio Kav. 3–5
Jakarta 12940
Indonesia

Tel: +62 21 2988 5959
Email: enrico@bepartners.co.id
URL: www.bepartners.co.id

Enrico Iskandar is a partner of Bagus Enrico & Partners, a firm which advises companies in corporate and commercial transactions, with an emphasis on mergers and acquisitions, corporate restructurings, property, hotels and real estate, technology, and media and telecommunications.

In his technology, media and telecommunications practices, Enrico has worked on a broad range of transactional, advisory and contentious matters, and regularly advises on regulatory issues on telecommunications, networks and satellite operations, data protection/privacy, encryption, outsourcing, IT contracts, and e-commerce (online securities, trading and advertising). Enrico's considerable experience in relation to technology, media and telecommunications has enabled him to steer investors through the inherent practical and regulatory hurdles.

As part of recognition of his representation for multinational clients in Information Technology, Telecommunication and Media, Enrico's team has been recognised by the ***Asia Pacific Legal 500 2017*** edition as Indonesia's **1st Tier** law firm in **IT & Telecoms practice**. He also been selected in the **2013**, **2014**, **2015** and **2016** editions of ***The International Who's Who Legal***, as a leading individual in Information Technology practice, and in the **2014** and **2015 editions** of the same publication as a leading individual in **Telecoms & Media practice**.

Bimo Harimahesa
Bagus Enrico & Partners
DBS Bank Tower, 17th floor, Suite 1701
Jl. Prof. Dr. Satrio Kav. 3–5
Jakarta 12940
Indonesia

Tel: +62 21 2988 5959
Email: bimo@bepartners.co.id
URL: www.bepartners.co.id

Bimo is a principal associate of Bagus Enrico & Partners. Mainly focusing on technology, media and telecommunication areas, Bimo has been actively involved in advisory for regulatory issues across TMT aspects including telecommunication and networks operation, data privacy protection, cloud services, and e-commerce industries.

Bimo also regularly advises the firm's clients within a wide spectrum of corporate and commercial matters on various sectors; namely, mergers and acquisitions, property, hotels and real estate, and employment, as well as advising various mainstream corporate clients.

BAGUS ENRICO & PARTNERS
COUNSELLORS AT LAW

Bagus Enrico & Partners ("**BE Partners"**) is one of Indonesia's leading corporate and commercial law firms. Founded by professionals who are recognised for their experience in handling various notable transactions in Indonesia, BE Partners continues its growth with an equal commitment to its reputation as a "boutique practice [which] focuses on client service", and provides its domestic and international clients with high-quality advice which is commercially focused and personally delivered.

BE Partners has received recognition from the main legal market reviewers. Some of international and the most respected reviewers have placed BE Partners' team as Indonesia's leading professionals in various practices. BE Partners' reputation in diverse aspects of Indonesian law, especially in relation to corporate/commercial law, banking, finance and insurance, mergers and acquisitions, IT, media and telecommunications, energy and resources, property, hotels and real estate, as well as infrastructure, is outstanding.