Indonesia


Enrico Iskandar


Bimo Harimahesa

Bagus Enrico & Partners

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under Law No. 11 of 2008 regarding Information and Electronic Transactions, as lastly amended by Law No. 19 of 2016 ("EIT Law"), hacking constitutes a criminal offence, which is subject to various penalties depending on the intention and the means of hacking. In general, the EIT Law stipulates that any person who, without lawful authority or against the law, intentionally accesses another person's electronic system shall be sentenced to maximum imprisonment of six years and/or a maximum fine of Rp.600 million. As for hacking for the purposes of obtaining electronic information and/or electronic records, this criminal act is punishable with a maximum imprisonment of seven years and/or a maximum fine of Rp.700 million. Meanwhile, hacking by means of breaching, infiltrating, or breaking through security systems is punishable with a maximum imprisonment of eight years and/or a maximum fine of Rp.800 million.

Denial-of-service attacks

There is no specific provision under the EIT Law which regulates Denial of Service attacks ("DoSA"). However, DoSA may be classified as system interference which may result in faults in the operation of electronic systems under the EIT Law, and is punishable with a maximum imprisonment of 10 years and/or a maximum fine of Rp.10 billion.

Phishing

Generally, phishing can be considered as a fraudulent act under the Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana* – "KUHP"), which is subject to a maximum of four years of imprisonment. Depending on the phishing methods being used, a phisher may also be charged with the provisions under the EIT Law. For instance, phishing through 'covert redirect', or unlawful transfer of electronic information, is punishable with a maximum imprisonment of 12 years and/or a maximum fine of Rp.12 billion under the EIT Law.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

There is no specific regulation in Indonesia which regulates the infection of IT systems with malware. However, under the EIT Law, this action may be classified as system interference. See the answer in respect of DoSA above for details on the applied sentences.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Under the EIT Law, possession of computer hardware or software that is designed or developed specifically to facilitate cybercrime is punishable with a maximum imprisonment of 10 years and/or a maximum fine of Rp.10 billion. Additionally, the restriction under the EIT Law is not only limited to possession or use only, but also stretched to the production, sale, organisation to be used, import, distribution, and even provision of such cybercrime tools.

Identity theft or identity fraud (e.g. in connection with access devices)

Identity theft or identity fraud may be considered as unlawful manipulation of personal data with the intention of misusing a certain individual's identity. Such criminal act may be subject to Article 35 of the EIT Law and is punishable with a maximum imprisonment of 12 years and/or a maximum fine of Rp.12 billion.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Under the EIT Law, electronic theft is categorised as hacking or unlawful transfer of electronic information and/or electronic records, which shall be subject to a maximum imprisonment of nine years and/or a maximum fine of Rp.3 billion. Moreover, Law No. 30 of 2000 regarding Trade Secrets ("Law No. 30/2000") stipulates that breach of confidential information, including trade secrets, by an employee is punishable with a maximum imprisonment of two years and/or a maximum fine of Rp.300 million, whilst Law No. 28 of 2014 regarding Copyright ("Copyright Law") stipulates that criminal copyright infringement is punishable with a maximum imprisonment of four years and/or a maximum fine of Rp.1 billion.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

The EIT Law also prohibits any unlawful alteration, addition, reduction, transmission, tampering with, deletion, moving, and covering of any electronic information and/or electronic records owned by another person or public. Any criminal act related to the foregoing is punishable with a maximum eight years of imprisonment and/or a maximum fine of Rp.2 billion. If such act resulted in the divulgement of confidential electronic information and/or electronic records in the public sphere with inaccurate data, the offender may be sentenced to a maximum of 10 years of imprisonment and/or a maximum fine of Rp.5 billion.

Failure by an organisation to implement cybersecurity measures

Under Indonesian law, the failure of an organisation or corporate entity to implement cybersecurity measures would not lead to the imposition of criminal sanctions. On a side note, the EIT Law stipulates that if a criminal offence in cybersecurity sector is committed by a corporate entity, the criminal sanctions shall be applied with two-thirds of the basic sentence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, all criminal sanctions stipulated under the EIT Law have extraterritorial application. Article 2 of the EIT Law stipulates that the EIT Law itself shall apply to any person who commits legal acts as governed by this law, both within and outside the jurisdiction of Indonesia, having legal effect within and/or outside the jurisdiction of Indonesia and that are detrimental to the interest of Indonesia.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The EIT Law provides exemptions for two actions that may not be considered as criminal offences, which are as follows:

a) data interception, if it is permitted and conducted by an authorised law enforcer for the purpose of law supremacy and national security; and

b) possession of cybercrime tools, if they are intended for research activities, testing and protection of the electronic system itself, insofar as the tools are possessed in a legal and lawful manner.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Depending on the cause of action, the occurrence of an Incident may lead to another criminal offence under Indonesian laws and regulations. For instance, unlawful manipulation of electronic information and/or electronic records for money laundering purposes is punishable with a maximum imprisonment of 20 years and/or a maximum fine of Rp.5 billion pursuant to Law No. 8 of 2010 on Eradication and Prevention of Money Laundering Crimes.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Cybersecurity

The Indonesian legal framework for cybersecurity is dispersed over a number of different regulations depending on the context of the Incidents. Nonetheless, the main reference for cybersecurity in Indonesia still refers to the EIT Law, which serves as the principal policy for electronic information in Indonesia.

Data Protection

In the event that the Incidents involves personal data, data protection provisions under Ministry of Communication and Informatics ("**MCI**") Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic System ("**MCI Regulation 20/2016**") shall apply. MCI Regulation 20/2016 requires all electronic system operators in Indonesia to store any personal data in its possession in an encrypted form, although there's no further stipulation on the encryption mechanism to be implemented. Further, MCI Regulation 20/2016 covers various aspects of personal data protection including an internal policy requirement in managing personal data, a notification requirement in the event of a data breach, and a reporting obligation for cross-border personal data transfer.

In addition, Government Regulation No. 82 of 2012 regarding the Implementation of Electronic Systems and Transactions ("**GR 82/2012**") requires the electronic system operator to maintain the confidentiality, integrity and availability of personal data, for which any use and/or disclosure of personal data is based on the personal data owner's consent and approval.

Intellectual Property

The Ministry of Law and Human Rights ("**MoLHR**") and MCI jointly issued Decree No. 14 of 2015 and No. 26 of 2015, respectively, regarding the Implementation of Closing Down Content and/or User Right to Access on Copyright Infringement and/or Related Rights in Electronic Systems. The joint decree stipulates, among others, a procedure on filing a report on copyright infringement in electronic systems, a verification procedure for filed reports, as well as aa procedure for closing down the content and/or access right related to copyright infringement.

Privacy of Electronic Communications

The privacy of personal electronic communications is guaranteed under Indonesian prevailing laws and regulations. Pursuant to the EIT Law, any person is prohibited to conduct any interception or wiretapping of electronic information and/or electronic records in certain computers and/or electronic systems of other persons without any consent and/or authorised by the owner. However, for law enforcement purpose, lawful interception is permitted and may be applicable.

Information Security

Depending on the sensitive data to be managed by an electronic system, it may be subject to certain information security provisions under Ministry of Communication and Informatics Regulation No. 4 of 2016 regarding Information Security Management Systems ("**MCI Regulation 4/2016**"). Please see the answer to question 2.2 for detailed information.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Under MCI Regulation No. 4 of 2016, electronic systems for public services are divided into three categories based on their risks, namely: (i) strategic electronic systems, which has a serious impact on public interest, public services, state administration continuity, or national security and defence; (ii) high-level electronic systems, which has limited impact for sectoral and/or regional interests; and (iii) low-level electronic systems, which does not fall under the categories of strategic and high-level electronic systems. Particularly for strategic

and high-level electronic systems, they are obliged to implement the SNI ISO/EIC 27001 standard and obtain a Information Security Management System Certificate. Such certification shall be issued by certification institutions that are acknowledged by the MCI. Failure to comply with this obligation will result in the imposition of administrative sanctions, i.e., written warning and temporary suspension of their Indonesian Domain Name.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The EIT Law and its implementing regulations use the term Electronic System Operator (*Penyelenggara Sistem Elektronik* – "**ESO**"), which has the meaning of any person, state administrator, corporate entity or community 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. With the broad definition of ESO, any organisations that operate an electronic system will be categorised as an ESO.

Under GR 82/2012, ESOs are required to implement several measures to protect their electronic system operational activity, among others:

- providing an audit trail for the purposes of monitoring, law enforcement, dispute settlement, verification, testing, incident response and mitigation;
- securing the components of its electronic systems;
- having and implementing a procedure and facility for securing its electronic systems to avoid disruption, failure, and loss;
- providing a security system, which includes a system and procedure for handling and preventing any cyber threats; and
- preserving the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information and/or electronic records that it maintains.

Further, specifically for ESOs that are related to public services, they are required to have a business continuity plan to anticipate any disturbance or disaster, as well as locate their Data Centre and Disaster Recovery Centre ("**DC/DRC**") within the territory of Indonesia for the purposes of law enforcement, protection, and implementation of state sovereignty over its citizens' data.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Particularly on the requirement of locating a DC/DRC within the territory of Indonesia, a conflict of laws issue may arise. Under Indonesian laws and regulations, an online marketplace that facilitates financial payments and/or transactions is considered an electronic system for public services; hence its provider may be obliged to locate its DC/DRC within the territory of Indonesia. However, if the online marketplace service is globally available and the provider is incorporated in a country that prohibits storage of data in overseas territory, DC/DRC of such provider is not able to be physically located within the Indonesian territory.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

GR 82/2012 stipulates that if electronic system failure or interference with serious effects caused by another party occurs, the ESO must secure the data and immediately report to the law enforcer or the relevant supervisory agency or sectoral regulator. However, GR 82/2012 does not further provide the nature and scope of information that is required to be reported, let alone any exemption for this requirement.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There are no prohibitions under Indonesian law for an ESO to share information related to Incidents or potential Incidents to another party, even if such party is located outside the Indonesian jurisdiction. Nonetheless, under MCI Regulation 20/2016, if the share of information involves disclosure of personal data to overseas, the ESO must firstly coordinate with MCI or the relevant supervisory agency or sectoral regulator. Further, consent from the personal data owner must firstly be obtained prior to the proposed transfer of personal data to either within Indonesia or abroad.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Any Incidents related to breaches of personal data must be reported to the personal data owner. In conveying such report, the relevant ESO must take into account the following requirements: (i) the report must include the reason or cause for the data breach's occurrence; (ii) the report may be delivered electronically provided that the relevant personal data owner has approved such way of delivery during the collection of his/her personal data; (iii) the ESO must 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 days after the data breach(es) came into realisation.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the response will not change due to the inclusion of the above-mentioned information.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The following bodies are responsible: (i) the Directorate General of Application Informatics of MCI, (ii) the Cyber Body and National Encryption Agency ("**BSSN**"), (iii) the Indonesia Security Incident Response Team on Internet and Infrastructure ("**ID-SIRTII**"), and (iv) any other relevant supervisory agency or sectoral regulator based on the ESO's business field.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Administrative sanctions apply, which may be taken in the forms of (i) a warning letter, (ii) administrative fines and/or (iii) suspension of business activity.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Enforcement actions are normally taken in the sectoral field, in particular the banking and insurance sector. We are aware of the fact that one of the insurance companies in Indonesia received a warning letter from the Financial Services Authority (*Otoritas Jasa Keuangan* – "**OJK**") to open up a data centre within the Indonesian territory. However, we have never been aware of any case in which a failure to meet the compliance requirements related to cybersecurity issues resulted in the imposition of administrative fines or suspension of business activity. Even during the Cambridge Analytica data scandal in early 2018, the MCI only sent a written warning and the Indonesian Parliament sent a summoning letter to Facebook regarding the personal data breach, yet no sanctions have been imposed on Facebook.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The information security requirements under GR 82/2012 and personal data protection under MCI Regulation 20/2016 are applicable to any ESO, regardless of its business sector. The most common deviation from the requirement under GR 82/2012 is applicable for any ESOs that are not related to public services, as they are not bound to mandatorily place their DC/DRC within the Indonesian territory. In addition, banking sectors may also be exempted from such requirement, provided that an approval from the relevant supervisory agency or sectoral regulator is obtained. Please see question 3.2 below.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) Financial Service

Use of information technology in the banking sector is regulated under OJK Regulation No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks ("**OJK Regulation 38/2016**"). OJK Regulation 38/2016 contains stricter compliance requirements for the use of information and technology in banking sectors compared to other business sectors. The following are examples of compliance requirements under OJK Regulation 38/2016 that are related to cybersecurity matters:

- forming an Information Technology Steering Committee, which at least comprises of (i) a director who oversees the IT working unit, (ii) a director who oversees the risk management working unit, (iii) the highest officer who leads the IT working unit, and (iv) the highest officer who leads the IT user working unit;
- performing a trial of the Disaster Recovery Plan for all critical applications and infrastructures in conformity with the result of the business impact analysis, at the latest once within a year;
- background check of criminal records during the recruitment of IT staff, including staff of the IT service provider, and network administrator or system administrator positions;
- the requirement to have an operational IT security procedure, which includes, among others, maintaining records of the antivirus and software versions that are being used;
- considering the formation of an Incidents Response Team in Information Security, in accordance with the bank's business complexity;
- within seven days after the event is identified, reporting any critical events, abuse, and/or criminal offences in the implementation of information technology which may and/or have caused significant financial losses and/or disrupt the bank's operational continuity, in the form stipulated by OJK; and
- the DC/DRC may be located outside the territory of Indonesia provided that an approval from OJK is obtained, which will be granted if, among others, personal data of the bank's customers and their respective transactions records are not involved.

Additionally, any electronic system operator involved in Electronic Money will be required to comply with the security standard for information systems under BI Regulation No. 20/6/PBI/2018 regarding Electronic Money ("**BI Regulation 20/2018**"). BI Regulation 20/2018 contains the following security standards:

- certification compliance and/or security standards and system reliability that are applied generally or stipulated by the Bank of Indonesia or a related agency;
- maintenance and improvement of the security technology;
- self-assessment of the information system in use at least once a year;
- conducting an information system audit by an independent security auditor at least once every three years or after any significant changes; and
- issuers of Electronic Money with a value limit of more than Rp.2.000.000 must increase their security standards through the use of two-factor authentication.

(b) Telecommunication

Telecommunication network providers are considered as ESOs for public services, and are thus required to implement the general requirements of information security under GR 82/2012. Please see the answer to question 2.3 above for the detailed requirements.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are no specific regulations in Indonesia which regulate the responsibility of the Board of Directors of a company to conduct all necessary actions in relation to prevent, mitigate, manage or respond to any Incidents. Nonetheless, directors are required, under Indonesian Company Law, to conduct management of the company in the best interest of the company with good faith and full responsibility. Therefore, a failure to prevent, mitigate, manage or respond to an Incident may be considered a breach of director's duties in the event that the failure resulted from the directors' fault or negligence. On a side note, specifically for the banking sector, one of the directors' duties is to establish an Information Technology Strategic Plan and Bank Policy for Implementation of Information Technology, in accordance with OJK Regulation 38/2016.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Only companies in the banking sector are imposed with the requirement to designate a CISO, submit a written Incident response, conduct a periodic assessment (including to its IT services providers), and perform a trial of their Disaster Recovery Plan.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

GR 82/2012 stipulates that if electronic system failure or interference with serious effects caused by another party occurs, the ESO must secure the data and immediately report to the law enforcer or the relevant supervisory agency or sectoral regulator. For listed companies, there are no specific requirements to disclose cybersecurity risks or Incidents in their annual report. They may, however, be required to include the occurrence of any issues which significantly affect the listed company's performance and/or stability.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Other than in the banking and financial sectors, there are no specific requirements related to cybersecurity matters that are applicable for listed companies in Indonesia.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Any civil actions that may be brought in relation to Incidents shall be based on breach of contract or tort. Particularly for tort, the EIT Law provides an underlying provision for any person, whose rights are infringed due to the unauthorised use of his/her personal data, to lodge a claim for damages.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

In 2013, a 19-year-old boy was sentenced to six months of imprisonment and charged with a fine in the amount of Rp.250,000 after he was found guilty of hacking into the official website of the Indonesian ex-president and committing illegal DNS redirection against the website.

In 2017, a man called Adi Syafitrah (with the alias M2404) was sentenced to one year and three months of imprisonment after he was found guilty of hacking into the official website of the Indonesia Press Council.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Any liability in tort cases will be subject to the amount of damages incurred by the claimant and its relation to the wrongful act.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out an insurance policy in relation to risks of Incidents as there is no prohibition regarding this matter under the Indonesian laws.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no regulatory limitations in providing insurance coverage against specific types of loss over Incidents.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There is no specific regulation on this matter under Indonesian law.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There is no specific regulation on this matter under Indonesian law.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

For the purpose of criminal offences in the IT sector, an investigator may conduct the following actions under the prevailing law and regulation:

a) Data Interception and Tapping

According to MCI Regulation No 11/2006 and the EIT Law, lawful interception and tapping may conducted by an authorised law enforcer for the purpose of law supremacy, national security, and criminal investigation. As for interception of mobile telecommunication networks and fixed telecommunication networks without cable infrastructure, the technical requirements for lawful data interception is further regulated under MCI Regulation No. 8/2014.

In relation to the Eradication of Terrorism Law No. 5 Year 2018, based on sufficient preliminary evidence, an investigator may conduct the following:

- Opening, checking, and impounding letters and shipments by post or shipping services that are related to terrorism law.
- Tapping phone conversation or other communication devices that may be used for preparing, planning, and carrying out criminal acts of terrorism, and also to detect someone related to, or a network of, terrorism.

The tapping mentioned above should be approved by the head of the relevant district court based on its jurisdiction. Except in emergency situations, an investigator may conduct tapping after the approval of head of district court. The tapping may be conducted for at most one year and can be extended once by at most one year. The resulting evidence of the tapping is confidential and may be used for the investigation of terrorism only.

b) Recording and Disclosing Any Data

Law No. 36 of 1999 regarding Telecommunication ("**Telecommunication Law**") and Government Regulation No. 52 of 2000 regarding Telecommunications Operation ("**GR 52/2000**") permit telecommunication services providers, for the purpose of criminal proceedings, to record any information delivered or received by it, as well as to provide any necessary information upon the following conditions:

- Written request from the Attorney General and/or Head of the Indonesian Police Force for certain criminal acts that are sentenced with five years' or more imprisonment, a life sentence, or the death penalty.
- Request from the lawful investigator for certain criminal acts pursuant to the prevailing laws and regulations.

The Telecommunication Law and GR 52/2000 state that any kinds of information may be recorded and disclosed for the purposes of criminal proceedings. Accordingly, this interception covers all types of communications facilitated by the relevant telecommunication services provider.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

The Telecommunication Law and GR 52/2000 stipulate that service providers must cooperate with the state during criminal proceedings by providing any necessary information. Consequently, should there be any encrypted information, the telecommunication services provider must cooperate with the law enforcer by providing the required encryption keys.

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
Fax: +62 21 2988 5958
Email: enrico@bepartners.co.id
URL: www.bepartners.co.id

Enrico Iskandar is a founding 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, 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 the 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 & 2018 edition*** as Indonesia's **1st Tier** law firm in ***IT & Telecoms*** practice. He has also been selected in the ***2013, 2014, 2015, 2016 2017 and 2018 editions*** of ***The International Who's Who Legal***, as a leading individual in ***Information Technology*** practice, and in the ***2014 and 2015 editions*** on 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
Fax: +62 21 2988 5958
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.

In the TMT sector, Bimo's recent representations include advising a major US-based technology company in the preparation of a global unified warranty template for the sales of its hardware products, assisting a UK-based technology company in advising a global privacy policy for the potential rollout of its intelligent household appliance, and regulatory requirements for the provision of IPVPN services licensing in Indonesia.

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 our 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 the most international and 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.