COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Indonesia

DATA PROTECTION & CYBERSECURITY

Contributor

H & A Partners in association with Anderson Mori & Tomotsune

Steffen Hadi

Partner | steffen.hadi@amt-law.com

Vicia Sacharissa

Associate | vicia.sacharissa@amt-law.com

Kalila Desi Jujane

Associate | kalila.desijujane@amt-law.com

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

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

INDONESIA
DATA PROTECTION & CYBERSECURITY

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

Presently, main regulations include:

a. Law No. 27 of 2022 on Personal Data Protection ("**PDP Law**"): main framework for the general privacy and data protection in Indonesia, whether electronically or physically, in any kind of activities (i.e. collection, process, utilization, etc.).
b. Law No. 11 of 2008 on Electronic Information and Transaction, as lastly amended by Law No. 1 of 2024 ("**EIT Law**"): regulates mainly on electronic transaction which also pertains, to certain extent, protection of personal data.
c. Government Regulation No. 71 of 2019 on the Implementation of the Electronic System and Transaction ("**GR 71/2019**"): one of the implementing regulations of EIT Law, which mainly governs Electronic System Operators ("**ESO**") and maintenance of electronic system in the context of personal data protection.
d. Minister of Communication and Informatics ("**MOCI**") Regulation No. 20 of 2016 on the Protection of Personal Data within the Electronic System ("**Regulation 20/2016**"): one of the implementing regulations of EIT Law which further elaborates personal data collection and their protection within electronic system.
e. MOCI Regulation No. 5 of 2020 on the Implementation of Electronic System in the Private Sector as lastly amended by MOCI Regulation No. 10 of 2021 ("**Regulation 5/2020**"): one of the implementing regulations of EIT Law, which further regulates the registration requirement for ESO.
f. Other institutional rules or circular letters (circular letters are not regulations per se but can be guidance to interpret the stance of authorities) issued by relevant institutions such as The National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara,* or "**BSSN**").

All present regulations pertaining to protection of personal data and electronic system in this context apply extraterritorially.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

Early in 2024, the recent amendment to EIT Law was enacted. Such amendment mainly governs the establishment of a number of additional regulatory frameworks on certification for electronic signature and documents, protection of underage person within electronic system, and expansion of prohibited actions such as defamation and doxing via the social media.

In addition, the Indonesian government is currently in a process to finalize and enact the draft Government Regulation on the Implementing Regulation of Law No. 27 of 2022 on Personal Data Protection ("**Draft PDP GR**"). Draft PDP GR will be the first implementing regulation of PDP Law which will provide further details on regulations pertaining personal data protection such as obligations of personal data controllers, personal data protection officers and elaboration on consent.

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

Yes, there are. Regulation 5/2020 mandates that an ESO must be registered in MOCI as evidenced by the issuance of ESO registration certificate.

While Regulation 5/2020 does not specify any exemption, Regulation 5/2020 sets out criteria of the ESO which must be registered:

i. ESOs that are regulated or under the supervision of certain government ministry/body; and/or
ii. ESOs that own any online portal, site, or application accessible from the internet that is used for:
iii. providing, managing, and/or operating the offer and/or trade of goods and/or services;
iv. providing, managing, and/or operating financial transaction services;
v. sending paid digital material or content through the data network, whether by way of downloading through a portal or site, by sending through email, or using other application to the user's device;
vi. providing, managing, and/or operating communication services including but not limited to short messages, voice or video calls, emails, and online conversation in the form of digital platform, online services and social media;
vii. search engine services, provision of electronic information in the form of writings, sounds, pictures, animation, music, videos, films, games, or any combination of the aforementioned items;
viii. processing of personal data for public service operational activities related to electronic transaction activities.

Given the broad-brushed criteria, it is not an uncommon perspective that any ESO with electronic systems that are accessible in Indonesia must be registered.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

The most common term used in Indonesian legislations is "Personal Data". There are several definitions of Personal Data, but with similar essence and underlying caveat as follows:

a. In PDP Law, GR71/2019 and Regulation 5/2020, Personal Data is defined as data regarding individuals who are identified or identifiable, whether by itself of in combination with other information, whether directly or indirectly, through the electronic system or non-electronically.
b. In EIT Law, Personal Data is defined as Certain Individual Data which is stored, maintained; its validity preserved and its secret protected.
c. In Regulation 20/2016, Personal Data is defined as certain individual data of which the truthfulness is stored, maintained and secured and which confidentiality is protected.

Pursuant to the PDP Law, personal data is further categorized into two: personal data of general nature, and personal data of specific nature. The latter consists of data and information pertaining to one's health, biometric data, genetics data, criminal records, children's data, personal finance data, and other data as may be regulated under the prevailing laws. Regulation 5/2020 uses the term "**Specific Personal Data**" to cover such data.

Meanwhile, EIT Law also recognizes the term "**Certain Individual Data**" which is further defined as any true and real information attached and identifiable, whether directly or indirectly, to specific individuals, and the use of which is subject to the laws and regulations.

The PDP Law also recognizes the term "**Information**". It is defined as information, statements, ideas, and signs that contain values, meanings, and messages; data, facts, and explanations that can be seen, heard, and read which are presented in various packages and formats in accordance with the development of information technology electronically and non-electronically.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered

entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

The general principles of personal data processing in Indonesia, among others, include:

(a) Limited and specific, lawful, and transparent.

Collection of personal data must be limited and specific (only pertains to personal data that are necessary), lawful (must be carried out by strictly adhering to the prevailing laws and regulations, such as obtaining express written consent) and transparent (full disclosure and access to personal data owner regarding their personal data on how the personal data is utilized or maintained).

(b) Specific in purpose.

Purpose to process personal data must be expressly informed to the personal data owner and must be observed when processing the personal data.

(c) Due observance to rights of personal data owner.

Personal data controller and processor have the full responsibility to abide and fulfill the rights of personal data owner (e.g. request to delete personal data must be respected).

(d) Accurate, complete, not misleading, up-to-date, and accountable.

The PDP Law stipulates that the personal data controller is obliged to ensure the accuracy, completeness, and consistency of personal data by verifying to the relevant personal data subject or the transferor of personal data.

(e) Strict protection of personal data.

The processing of personal data is carried out by protecting the security of personal data from any unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or loss of personal data.

(f) Due observance to retention period.

The general retention period for storage of personal data in the electronic system is 5 (five) years, but specific sectors may stipulate otherwise.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

As a rule of thumb, the collection and processing of personal data must be based on express consent. PDP Law, however, sets forth certain situations where consent is not needed is when the personal data is collected and process due to, among others, public or vital interests (e.g. tax purposes).

7. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Pursuant to the PDP Law, consent must be made in writing or any recorded form, electronically or non-electronically. Strictly speaking, the consent may not be implied or bundled with other matters which may obscure the context of the consent itself.

The consent form must at least include the following information:

a. legality of the personal data processing;
b. purpose of personal data processing;
c. types and relevance of the personal data which will be processed;
d. retention period of documents containing personal data;
e. details about the information that are collected;
f. period of personal data processing;
g. rights of the personal data subject.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

Processing of sensitive personal data is subject to the requirement on impact assessment and appointment of Personal Data Protection Officer ("**PDPO**"). Further elaboration on impact assessment, however, is yet to be regulated.

In general no, provided that the collection or disclosure

is based on lawful basis (e.g. consent).

9. How do the data protection laws in your jurisdiction address health data?

As a bottom line, health data is considered as personal data, hence subject to the regulations pertaining to personal data protection.

Management of health data in specific relevant institution, however, is regulated under Minister of Health ("**MOH**") Regulation No. 24 of 2022 on Medical Record ("**Regulation 24/2022**") which governs the management of electronic health data (mainly in the form of medical record). This regulation mandates that every health service facility must implement electronic medical record. The electronic system used to manage the medical records can be the electronic system which is developed by (i) the MOH (through the ministry); (ii) the health service facility by itself; or (iii) in cooperation with ESO. For point (ii) and (iii), the electronic system must be connected/interoperability with MOH's electronic system. Their electronic system must also be registered in MOH's database. The retention period for medical records is 25 (twenty-five) years.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

No, kindly refer to our responses above.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

Yes, EIT Law and PDP Law recognizes the protection of personal data of underage person. As a rule of thumb, consent provided by underage person must be supported with consent from the parents or guardian.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

Yes, EIT Law sets forth a series of prohibited actions that pertain to only safety which include, among others, prohibition pertaining to illegal distribution of unlawful content, defamation, false information, etc.

Violation against such prohibition will be imposed with penal sanctions in the form of imprisonment (ranging from maximum 2 (two) to 12 (twelve) years) and fines (ranging from maximum IDR600,000,000 (six hundred million Rupiah) to IDR12,000,000,000 (twelve billion Rupiah).

ESO is also imposed with obligations to supervise and maintain its electronic system to comply with the requirements regarding online safety.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

Online safety in general is under the auspices of MOCI (alongside BSSN to some extent), as it is under the same umbrella with personal data protection. Upon occurrence of crimes, these authorities will work in tandem with the police and general prosecutor.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

Yes, Draft PDP GR stipulates a more detailed obligation for the personal data controller in relation to personal data of children and disabled people.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

Yes, personal data protection regulations in Indonesia impose both requirements.

Data protection by design can be seen in GR 71/2019 which mandates any ESO (and by extension, personal data controllers in the electronic system) to maintain the proper and sufficient technical and organizational measures designed to implement the data protection

principles effectively.

Data protection by default is shown mainly by the requirements in PDP Law, as highlighted in one of the principles mentioned in point 5 above.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Yes. PDP Law stipulates that personal data controllers are required to record all personal data processing activities. GR 71/2019 and Regulation 20/2016 also stipulates that ESOs (by extension, personal data controllers in the electronic system) are required to provide audit trail of all activities conducted within the electronic system, including the processing of personal data.

In practice, the recordation mechanism of an electronic system is actually being implemented during the inception of electronic system itself. To certain extent this might amount to the fulfilment of the above requirements (subject to further assessment on the framework of the electronic system itself).

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Yes. The data protection law stipulates that personal data controller must keep one's personal data for no less than the retention period of 5 (five) years, unless the personal data subject requests otherwise. Some sectors may also stipulate a longer retention period, such as medical records which must be retained for at least 25 (twenty-five) years.

The disposal/destruction obligation applies in certain situation such as request from personal data owner and expiry of retention period.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

Some situations where consultation is required or encouraged is prior to the exercise of cross-border personal data transfer and failure of personal data protection in an electronic system.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk assessments typically carried out?

Yes. ESOs in general must carry out risk management measurement against any losses or damages toward their electronic system, especially if the personal data processing is considered as high risk activities (e.g. it includes automated decision, compilation of personal data as a bundle, etc.). Such risk management is done by analyzing the possible risks and formulating mitigation steps to overcome any disturbances, threats, and obstacles against their electronic system.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and what are their legal responsibilities?

Yes, a personal data controller must appoint PDPO if:

a. the personal data processing is done for public interest;
b. the personal data controller's main activity has a nature, scope, and/or purpose that requires regular and systematic supervision for big-scale personal data; and
c. the personal data controller's main activity consists of big-scale personal data processing for specific personal data and/or personal data related to criminal records.

Pursuant to PDP Law, PDPO's duties include in:

a. informing and providing advice to the personal data controller/processor to comply with the PDP Law;
b. supervising and ensuring compliance to the PDP Law and the personal data controller/processor's policies;

c. providing advice regarding personal data processing impact assessment and supervise the personal data controller/processor's performance;
d. coordinating and acting as liaison officer for issues related to personal data processing.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

Yes. Pursuant to GR 71/2019, ESOs must provide, educate, and train personnel who are in charge of security and protection of facilities and infrastructures of the electronic system.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Yes. For example, if someone accesses a website which uses cookie or utilize personal data, then the website must request consent from the individual (it can be in the form of pop-up messages). Since there are extensive matters which must be informed to personal data owner, a consent form is usually preceded by a privacy notice—at the end of the privacy notice, the individual can agree to the use of personal data.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

Yes. The PDP Law defines "personal data controller" as every person, public agency, and international organization that acts individually or jointly in determining purposes and exercising control over the processing of personal data. Meanwhile, "personal data processor" is every person, public agency, and international organization that acts individually or jointly in personal data processing on behalf of a personal data controller. Generally, personal data processor is appointed by personal data controller to carry out processing of personal data.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

Yes, any obligation of the personal data controller extends to the personal data processor.

The prevailing laws are silent on this. However, it is worth noting that the current Draft PDP GR elaborates further on the items to be stipulated in the contract terms with processors of personal data.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

No, there are not.

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

With regard to automated decision-making or profiling, although not prohibited or restricted per se, PDP Law sets out that personal data subjects are entitled to object to decision-making actions based solely on automated data processing including profiling that has a significant impact on personal data subjects. The PDP Law defines profiling as any activity to identify an individual, including but not limited to the employment history, economic conditions, medical records, personal preferences, interests, aptitudes, behavior, location, or movements of the data subject.

Aside from the above, provisions related to monitoring, tracking or cookies will subject to general provisions regarding personal data protection (e.g. necessity of consent, etc.).

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are

these terms or any similar terms defined?

As a bottom line, when personal data is involved it must be comply with personal data protection regulations.

Specifically, Government Regulation No. 80 of 2019 on Trade by Electronic Systems ("**GR 80/2019**") regulates electronic marketing. Electronic marketing must be made based on good faith and must comply with the applicable consumer protection and advertising regulations. Electronic marketing can be made through (i) registered mail; (ii) email; (iii) online sites; (iv) electronic media; or (v) other electronic communication channels.

The parties conducting the electronic marketing must explain the technical mechanism and substance of the terms and conditions of giving approval electronically. The offers are accepted if the receiving party has agreed to the given terms and conditions.

Electronic offers are valid and binding after a clear and specific statement of intention or will in the offer and terms and conditions in an honest, fair, and balanced (fair) bidding manner, and certain time restrictions.

In certain business sectors, such as banking and financial services , marketing is regulated further under their industry-specific rules.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

Indonesian laws do not specifically regulate sale of personal data.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

Please refer to our response in Number 27.

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

Biometric data falls under the classification of specific personal data (kindly refer to our response in Number 8 above).

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

Data protection laws in Indonesia are silent on AI.

Nonetheless, AI is regulated in the non-regulatory institutional guidelines through MOCI Circular Letter No. 9 of 2023 on Ethics of Artificial Intelligence ("**Circular 9/2023**").

The Circular 9/2023 provides guidance on the implementation of AI in order to comply with ethics including inclusivity, humanity, privacy and personal data security, accessibility, transparency, credibility and accountability, personal data protection, sustainable environmental development, and intellectual property.

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

Transfer of personal data outside Indonesia is allowed with the following requirements:

a. ensure that the recipient country has an equal or higher level of personal data protection than what is stipulated in the PDP Law;
b. ensure that there is an adequate and binding personal data protection; and
c. must obtain the consent of the personal data subject.

In addition, notification to MOCI is required prior and after the conclusion of such transfer. Although the regulations are silent on the procedure of such notification, MOCI has internally issued the format notification letter for this process.

33. What security obligations are imposed on data controllers and processors, if any, in your jurisdiction?

In essence, personal data controllers owe the obligations to protect personal data as mandated by data protection laws in Indonesia. Such obligations are translated into various specific requirements, among others which have been elaborated in our responses herein. Furthermore, if personal data controllers are also ESOs, they are subject to the extensive regulations pertaining to electronic system which are mainly regulated in GR 71/2019.

Separately, personal data processors, as parties appointed by and acting on behalf of personal data controllers, must also carry out the obligation to protect the security of personal data stipulated under the data protection laws, with some specific requirements under PDP Law as follows:

a. personal data processors shall carry out personal data processing based on the instructions of personal data controllers in accordance with the law;
b. the processing of personal data carried out by personal data processors at the behest of personal data controllers falls under the responsibility of personal data controllers;
c. personal data processors may involve other personal data processors in carrying out their duties after obtaining written approval from personal data controllers; and
d. in the event that the personal data processor carries out the processing of personal data outside the orders and purposes set by the personal data controller, the personal data processing shall be the responsibility of the personal data processor.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a “security breach”?

Yes. PDP Law defines a “security breach” as “failure of personal data protection”. Furthermore, “failure of personal data protection” shall mean as a failure to protect a person’s personal data in terms of confidentiality, integrity, availability of the personal data, including security breaches, whether international or unintentional, leading to destruction, loss, alteration, disclosure, or unauthorized access to the personal data which are being sent, stored or processed.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

Yes, in addition to data protection laws, some sectors are also subject to industry-specific regulation such as regulations in banking and financial sectors through Bank of Indonesia regulations and Financial Services Authority regulations.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

In the event of a failure to personal data protection, the personal data controller must provide written notification to personal data subject and the agency no later than 3 x 24 hours since the failure occurred.

The written notification shall at least contain:

a. the disclosed personal data;
b. when and how the personal data are disclosed; and
c. efforts to handle and recover from the disclosure of personal data by the personal data controller.

In the event that such breach interferes with public services and/or has serious impact on the public interest, the personal data controllers must publish written notification to the public regarding the failure of personal data protection.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

No. However, as a reference, one may refer to BSSN Regulation No. 4 of 2021 on Guidelines for Information Security Management of Electronic-Based Government Systems and Technical Standards and Security Procedures for Electronic-Based Government Systems (“**BSSN Regulation 4/2021**“). Although BSSN

Regulation 4/2021 is only relevant for governmental system, it provides guidelines in dealing with cybercrime against government electronic systems by taking the following steps:

a. identifying the source of the attack;
b. analyzing information related to subsequent incidents;
c. prioritize incident handling based on the level of impact;
d. documenting evidence of incidents that occur; and
e. mitigate or reduce the impact of electronic-based government system.

Separately, for cybercrime or cyberattacks that threaten national security, the Ministry of Defense ("**MOD**") issued Regulation No. 82 of 2014 on Cyber Defense Guidelines ("**Regulation 82/2014**") which provides cyber defense guidelines. However, Regulation No. 82/2014 only serves to develop military cyber defense capacities, developed and implemented by the MOD for the Indonesian National Armed Forces ("**TNI**").

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

Yes. Indonesia government established BSSN based on Presidential Regulation No. 28 of 2021 on BSSN. BSSN is delegated with authorities to carry out duties in the field of cyber security and coding.

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

Yes, as set out under PDP Law, summarized below:

a. the right to obtain information regarding identity clarity, basis of legal interest, purpose of requesting and using personal data, and accountability of parties that request personal data;
b. the right to complete, update and/or correct errors and/or inaccuracies in personal data regarding themselves in accordance with the purpose of the personal data processing;
c. the right to access and obtain a copy of personal data regarding themselves in accordance with provisions of laws and regulations;
d. the right to end processing, delete, and/or destroy personal data regarding themselves in accordance with provisions of laws and regulations;
e. the right to withdraw consent to the processing of personal data regarding themselves that has been given to a personal data controller;
f. the right to object a decision-making action that is based solely on automated processing, including profiling, which has legal consequences or have a significant impact on personal data subjects;
g. the right to delay or limit the personal data processing proportionally with the purpose of personal data processing;
h. the right to sue and receive compensation for violations of the processing of personal data regarding themselves in accordance with provisions of laws and regulations; and
i. the right to obtain and/or use personal data regarding themselves from personal data controller in a form that is in accordance with the structure and/or format commonly used or readable by an electronic system.

For the exemption against the rights of personal data subject referred above, please refer to our answer in Number 10.

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

Both. If the violation of rights amount to criminal action, the individual may file a report to police. On the other hand, the individual may also claim for monetary damages through civil lawsuit (kindly refer further to our responses in Number 41).

In addition, personal data subjects are allowed to submit personal data breach report to MOCI. MOCI also facilitates the settlement of disputes between personal data subjects and personal data controllers and/or personal data processors outside of the court.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Yes, the individual may file a civil lawsuit to the court

(whether through tort or breach of contract legal institution). Such rights are stated expressly in PDP Law and Regulation 20/2016.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Yes. Kindly refer to our response in Number 41.

In general, immaterial damage (e.g. injury to feelings, emotional distress or its equivalent) will only be considered if it involves death, slander or bodily harm. Aside from these situations, immaterial damage will subject to strict scrutiny by the court.

43. How are data protection laws in your jurisdiction enforced?

Generally, there is no special treatment for the enforcement of data protection laws. For instance, violation of laws which amount to crime will be investigated and prosecuted through normal procedures. MOCI as the issuer of several regulations will also have the authorities to impose administrative sanctions to certain business such as ESO. Separately, civil lawsuit may also be claimed for any civil losses suffered by personal data subject.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

PDP Law and EIT Law impose criminal sanctions in the form of imprisonment and fines. In the PDP Law, the maximum imprisonment is 6 (six) years and the maximum fine is IDR6,000,000,000.00 (six billion Rupiah), while in the EIT Law the maximum imprisonment is 12 (twelve) years and the maximum fine is IDR12,000,000,000 (twelve billion Rupiah). There are also additional penalties in the form of confiscation of profit and/or property as a result of a criminal offense and indemnification.

Corporations are also recognized as wrongdoers with additional sanctions as follows:

a. confiscation of profits and/or assets obtained or as a result of a criminal offense;
b. suspension of all or part of the corporation's business;
c. permanent prohibition to perform certain actions;
d. closure of all or part of the place of business and/or activities of the corporation;
e. forced to carry out obligations that have been neglected;
f. payment of compensation;
g. revocation of license; and/or
h. dissolution of the corporation.

There are also administrative sanctions ranging from written warning to fines.

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

Currently, no.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Yes. Similar to other situations, any order issued by the regulators (in this case, mainly MOCI) may be appealed to the administrative court. Court decision, however, will need to be appealed by using judicial appellate avenue available (e.g. appeal, cassation, etc.).

47. Are there any identifiable trends in enforcement activity in your jurisdiction?

While court decisions for lawsuits pertaining to data protection are still lacking, the trends of personal data leakage by various institutions have not seen significant decrease. Significant roles of MOCI and law enforcers on data protection, however, could still be seen, albeit slightly infrequent.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

We are not aware of any review on the proposals to reform data protection laws. This is quite understandable given that PDP Law itself is just recently enacted with transitionary period of two year (from 2022). The

attention lies instead on the implementing regulations of PDP Law (including Draft PDP GR) which many believe, could provide definitive technical elaborations on the regulations pertaining data protection.

Contributors

Steffen Hadi
Partner
steffen.hadi@amt-law.com

Vicia Sacharissa
Associate
vicia.sacharissa@amt-law.com

Kalila Desi Jujane
Associate
kalila.desijujane@amt-law.com