Legal 500
Country Comparative Guides 2025

Indonesia
TMT

Contributor

ABNR Counsellors at Law

Agus Ahadi Deradjat

Partner | aderadjat@abnrlaw.com

Mahiswara Timur

Senior Associate | mtimur@abnrlaw.com

Dhan Kaur

Associate | dkaur@abnrlaw.com

Natasya Amalia

Associate | namalia@abnrlaw.com

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

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

Indonesia: TMT

1. Software – How are proprietary rights in software and associated materials protected?

These are protected by copyright under Law No. 28 of 2014 on Copyright ("**Copyright Law**"). Software is defined as a computer program (a set of instructions expressed as language, code, schematics, or an order intended to make a computer perform a certain function or achieve a certain result), which is included as an object of copyright protection. The creators are afforded automatic copyright protection for 50 years from first announcement (*as registration is not a pre-requisite for copyright protection*).

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

In the absence of an agreed contractual provision, the software developer, consultant, or other party will be entitled to ownership of the propriety rights in the newly created software. This is based on the Copyright Law, which mandates that the creator of a work is the automatic owner of copyrighted work created by them, unless agreed otherwise.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

Yes, these are governed under Law No 11 of 2008 on Electronic Information and Transactions, as lastly amended by Law No. 1 of 2024 ("**EIT Law**") and Government Regulation No. 71 of 2019 on the Provision of Electronic Systems and Transactions ("**GR 71**"). The following are prohibited in relation to the operation of software/computer systems:

a. intentionally and illegally broadcasting, displaying, distributing, transmitting, and/or making accessible electronic information or documentation with content that violates decency, promotes gambling, is offensive or defamatory, or can extort/threaten people;
b. intentionally attacking the dignity or reputation of another person by accusing something, with the intention to make such matter be publicly known in the form of electronic information and/or electronic documents carried out through the electronic systems;
c. intentionally and illegally distributing and/or transmitting electronic information and/or electronic documents with the intention to unlawfully benefit themselves or others, forcing a person with threats of violence, threats of defamation or threats to reveal secrets to: (i) provide goods, which partly or wholly belong to that person or belong to another person, or (ii) provide loan, make acknowledgment of a debt, or write off receivables;
d. intentionally and illegally distributing and/or transmitting false or misleading news, resulting in consumer losses in electronic transactions;
e. intentionally and illegally spreading information intended to incite hatred or hostility towards certain individuals or groups of people based on their race, nationality, ethnicity, skin color, religion, belief, gender, mental disability or physical disability;
f. intentionally disseminating electronic information and/or electronic documents which they know contain false notification that cause riot in the society;
g. intentionally and illegally sending electronic information or electronic documentation that contains threats of violence or intimidation directly to the victim;
h. intentionally and illegally or unlawfully accessing in any way a computer or electronic system: (i) that belongs to another person, (ii) in order to obtain electronic information or documentation, or (iii) by violating, breaching, bypassing, or hacking a security system;
i. intentionally and illegally or unlawfully (i) intercepting or tapping electronic information or documentation held in a computer or electronic system that belongs to another party, or (ii) intercepting the transmission of non-public electronic information or documentation from, to, and in a computer or electronic system that belongs to another party, that may or may not alter, delete, or terminate electronic information or documentation being transmitted;
j. intentionally and illegally or unlawfully in any way: (i) changing, adding to, reducing, transmitting, damaging, omitting, moving, or concealing electronic information or documentation that belongs to another party or is

owned by the public, or (ii) moving or transferring electronic information or documentation to an electronic system of an unauthorized person;
k. intentionally and illegally or unlawfully take action that disrupts an electronic system or renders an electronic system inoperable;
l. intentionally and illegally or unlawfully producing, selling, procuring for use, importing, distributing, providing, or owning: (i) computer hardware or software that is designed or specifically developed to facilitate the actions referred to in points (a) to (h) above, or (ii) a computer password, access code, or the like, that is intended to provide access to an electronic system in order to facilitate the action referred to in points (a) to (h) above;
m. intentionally and illegally or unlawfully manipulating, creating, altering, omitting, or damaging electronic information or documentation in such a way that it appears to be genuine;
n. intentionally and illegally or unlawfully committing an act referred to in points (a) to (i) above that causes losses to another person;
o. intentionally committing a prohibited act referred to in points (a) to (k) outside Indonesian territory against an electronic system located within Indonesian jurisdiction.

Further, the recently issued Law No. 1 of 2023 ("**New Criminal Code**") stipulates that the following conduct will be subject to criminal sanction:

a. to unlawfully listen to, record, divert, modify, inhibit, or take note of the transmission of electronic information or documentation that is confidential, either by using a wired or wireless communications network;
b. to broadcast or disseminate the results of a discussion, or recording the above;
c. intentionally and illegally or unlawfully accessing the computer or electronic system of another person in any way;
d. intentionally and illegally or unlawfully accessing a computer or electronic system in any way for the purpose of obtaining electronic information or documentation;
e. intentionally and illegally or unlawfully accessing a computer or electronic system in any way by violating, bypassing, exceeding, or hacking its security system;
f. without permission, using or accessing a computer or electronic system in any way, with the intention of obtaining, altering, damaging, or eliminating information on national defense or international relations that may result in interference or harm the state or its relationship with the subjects of international law;
g. without permission, carrying out action that damages transmissions from programs, information, codes or orders protected by the state;
h. without permission or exceeding authority, using or accessing a computer or electronic system, either from within or outside the country, to obtain information from a computer or electronic system that is protected by the state;
i. without permission, using or accessing a government-owned computer or electronic system;
j. without permission or exceeding authority, damaging a state-protected computer or electronic system;
k. without permission or exceeding authority, damaging a computer or electronic system that is dedicated for community use;
l. affecting or disrupting the operation of a government computer or electronic system;
m. disseminating, trading, or utilizing an access code or similar input that can bypass computers or electronic systems, with the intention of misusing a government-used or -protected computer;
n. harming international relations via public messages by damaging a computer or other electronic system that is protected by the state and located within Indonesian jurisdiction;
o. without permission or exceeding authority, using or accessing a computer or electronic system in order to misuse for personal gain financial information from the central bank, a banking institution or financial institution, credit card issuer, payment card or a report containing personal financial data of a customer;
p. without permission, misusing data or accessing in any way credit card or payment card data belonging to other persons in electronic transactions for personal gain;
q. without permission or exceeding authority, misusing or accessing a protected computer or electronic system of the central bank, or a banking or financial institution for personal gain; or
r. disseminating, trading, or utilizing access codes or similar information that may be used to bypass a computer or electronic system with the intention of causing disruption that affects the electronic systems of the central bank, a banking or financial institution, and commercial activity within and outside the country; or
s. illegally using or accessing a computer or electronic system in any way, with the intention of obtaining, altering, damaging, or deleting government-owned information that must remain confidential or be protected.

Please note that the New Criminal Code is still under a 3-year grace period, thus, it would be in full force and effect

in January 2026.

4. Software – To the extent not covered by (3) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

No: in essence, the use (and misuse) of software/computer systems is mainly subject to the provisions of the EIT Law and New Criminal Code (upon the lapse of the grace period).

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

Generally, the provision of software between a vendor and customer is subject to the laws and regulations cited in (1) above, except for sector-specific regulations (which are determined by the customer's business activities).

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes, in practice, this is typical. The market standard level of cap depends on type of software, license/subscription fee, and the purpose of the software. It is very common that the limitation would be based on the license/subscription fee paid by the customer to the software provider.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

Confidentiality breaches, data protection breaches, breaches of applicable law, wilful or deliberate breaches are typically excluded from a financial cap on a software vendor's liability to a customer, or is subject to a separate, enhanced cap in a separate, negotiated software transaction.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

Currently, this is not yet the norm in Indonesia. However, this arrangement is not restricted under Indonesian laws, and there are various providers offering source codes escrow services. In our observation, the source codes escrow services are usually engaged for critical and high-valued software development.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

No, there are none.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

Other than the law cited in (1) above, IT outsourcing transactions are subject to sectoral laws (which are determined by a customer's business activities). For instance, IT outsourcing in the financial services sector is subject to several requirements under the Financial Services Authority, "**OJK**") and Bank Indonesia ("**BI**") regulations, which are:

- OJK Regulation No. 11/POJK/03/2022 on Implementation of Information Technology by Commercial Banks;
- OJK Circular Letter No. 21/SEOJK.03/2017 SEOJK on the Implementation of Risk Management in the use of Information Technology in Public Banks ("**SEOJK 21**");
- OJK Regulation No. 4/POJK.05/2021 on the Implementation of Risk Management in Using Information Technology by Non-Bank Financial

Services Institutions (*partially revoked by OJK Regulation No. 10/POJK.05/2022 on Peer-to-Peer Lending*); and
- BI Regulation No. 23/6/PBI/2021 on Payment Systems Providers.

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

Generally, individual staff are protected by Article 1367 Indonesian Civil Code, which provides that an individual will be responsible for damage that they have caused, as well as the action of those they supervise, or matters that are under their supervision. This includes employers and those assigned to manage the affairs of other individuals, who must take responsibility for damage caused by their subordinates in the course of duties assigned to them. However, this provision only provides protection against civil liability. Thus, individual staffs can still be subjected to criminal liability with regard to services they performed.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

Telecommunications networks and services are covered under the following laws:

Laws	Purpose
Law No. 36 of 1999 on Telecommunications, as amended by Government Regulation In Lieu of Law No. 2 of 2022 on Job Creation, (which has been ratified as Law No. 6 of 2023) ("**Telco Law**")	Core legislation that governs the telecoms sector. It sets out a telecoms sector regulatory framework, including general provisions on types of entity that are telecoms providers, a classification of telecoms networks and services, and sanctions.
Government Regulation No. 52 of 2000 on the Operation of Telecommunications, partially revoked by Government Regulation No. 46 of 2021 on Posts, Telecommunications, and Broadcasting	Implementing regulations of the Telco Law. Which introduces new classifications on telecoms networks and services, provision of special telecoms, resale of telecoms services, licensing, interconnection, tariffs, and universal service obligations.
Government Regulation No. 46 of 2021 on Posts, Telecommunications, and Broadcasting	
Ministry of Communications and Information Technology ("**MCIT**") Regulation No. 01/PER/M.KOMINFO/01/2010 on the Operation of Telecommunications Networks, amended several times, last by MCIT Regulation No. 5 of 2021 on the Operation of Telecommunications	Licensing and operational requirements for telecoms networks.
MCIT Regulation No. 14 of 2025 on Provision of Special Telecommunications for the Needs of Government Agencies or Legal Entities	Licensing and operational requirements for special telecoms (i.e., telecommunications for own purposes, research, or government agencies).
MCIT Regulation No. 13 of 2019 on the Operation of Telecommunications Services, amended several times, last by MCIT Regulation No. 14 of 2021	Licensing and operational requirements for telecoms services.
MCIT Regulation No. 5 of 2021 on the Operation of Telecommunications	Requirements and obligations, including licensing, interconnection, tariffs, and universal service obligations for each type of telecoms network and service.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

Telecommunications operations are considered as a highly regulated sector in Indonesia under the authority of the Ministry of Communications and Digital Affairs ("**MOCD**", formerly known as the MCIT), which can only be performed by a licensed Indonesian legal entity. According to Law No. 36 of 1999 on Telecommunications ("**Telco Law**"), telecommunications operations are classified into:

- Telecommunications network operation, including:
  - Fixed telecommunications network operation;
  - Mobile telecommunications network operation; and
  - Satellite Telecommunications Operation;
- Telecommunications services operation, including:
  - Basic telephony services;
  - Value-added telephony services; and
  - Multimedia services;
- Special telecommunications operation.

Each of the above categories is further classified into sub-categories of telecommunications operation, based on the specific type of telecommunications products, which would determine the appropriate type of license. The licensing process in telecommunications sector includes administrative and technical process, including operational worthiness test which would ultimately determine the eligibility of the operator.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

Law	Purpose
Telco Law	Telco Law requires telecommunication service provider to maintain the confidentiality of information sent and/or received by their customers through their telecommunications networks and/or telecommunications services. For the purpose of criminal proceedings, telecommunications service providers are permitted to record transmitted and/or received information. They may disclose such information upon: a. receiving a written request from the Attorney General and/or the Chief of the Indonesian National Police concerning specific criminal cases. b. receiving a request from authorized investigators for certain crimes, in accordance with applicable legal provisions.
Regulation No. 5 of 2020 on Private Electronic Systems Operators ("**ESO**"), as amended by MCIT Regulation No. 10 of 2021 ("**MR 5**")	For non-conventional telecommunications operators, such as OTT messaging services operator, MR 5 provides specific procedure for the law enforcement authority requesting information with regard to criminal investigation, including request for traffic data, subscriber information, and communications data. The request can only be filed if related to a crime subject to: (i) at least 5 years imprisonment (ii) at least 2 years imprisonment, provided that the request is based on a court order. With regard to communications data, the request must be based on an official written request, accompanied with a court stipulation.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

Currently the Indonesian Government is formulating the technical standards governing Internet of Things (IOT) (which may include the technical standards on mobile communications and newer connected technologies) devices. Considering the industry is emerging and the SSO is yet to be established, in principle, mobile communications and newer connected technologies are governed under electronic information and transactions and the personal data protection regulatory regime. Additionally, we have noted that the government has adopted industry-acknowledged ISO standards for IOTs into Indonesian National Standards (SNI), such as SNI ISO/IEC 30141:2018, SNI ISO/IEC 21823-1:2019, and SNI ISO/IEC 19637:2016.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

The current technical standards on mobile communications and newer connected technologies are referring to SNI ISO/IEC 21823-1:2019. However, this standard has not been set as a mandatory standard. Thus, we have not seen significant impact on this aspect.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that govern data protection, including a brief explanation of the general purpose of those laws.

Law	Purpose
PDP Law	Core legislation that governs personal data protection. It includes, a classification of general personal data and specific categories of personal data, the lawful bases for processing personal data, data subjects' rights, classification of data controller and data processor along with their respective obligations and liabilities, cross-border data transfer, data breach notice requirement, Data Protection Impact Assessment requirements, appointment of a Data Protection Officer, and sanctions.
EIT Law	General rules on electronic information and transactions, including management of personal data applicable to the operation of electronic systems in any business field.
GR 71	General rules and requirements for the operation of electronic systems and the processing of personal data by Electronic Systems Operators ("**ESO**"). (*It provides only general provisions on data protection.*)
MR 20	More specific obligations on ESOs to protect personal data.
MR 5	Obligations on ESOs in private scope, including data protection measures.
Draft of Government Regulation on the Implementing Regulation of Law No. 27 of 2022 on Personal Data Protection ("**Draft GR**")	The Draft GR is expected to bring clarity on numerous aspects of the PDP Law, including but not limited to the notification procedures on personal data breaches and minimum requirements for personal data processing in various related documents. The Draft GR is expected to be enacted in 2024.

In addition to the above general regulations, additional personal data protection provisions under sector-specific regulations apply to specific fields of business (e.g., e-commerce, banking, financial services, and medical services).

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

The sanctions that can be imposed on non-compliance with data protection law encompass:

- administrative sanctions: verbal warning, suspension of activities, access blocking, culminating in a fine of up to 2% of the annual income/revenue (*but not yet clear whether this refers to worldwide annual revenue or only that generated in Indonesia*); and
- criminal sanctions: imprisonment of up to 5 years and/or a fine of up to IDR 50 billion (for corporations), as well as additional criminal sanctions such as dissolution (of a corporation).

In addition, the PDP Law allows data subjects to submit a civil claim against a data controller/processor if they suffer damages as a result of unlawful processing of their personal data (the maximum value of which has not yet been stipulated).

19. Data Protection – Do technology contracts in

your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

No, reference to external data protection regimes would only be included if the contract contains any elements that would trigger any of such external data protection regimes (e.g., involving foreign data controller/processor or involving the processing of foreign data subjects' personal data). Other than that, in our observations, technology contracts in Indonesia only refer to Indonesian data protection laws and regulations.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

Law	Purpose
EIT Law	The security of electronic system, electronic transactions, use of electronic signature, and general security of cyberspace.
GR 71	The implementing regulation of the EIT Law, which applies specifically to ESOs, including the security of hardware and software used by ESO.
Cyber and Crypto National Agency (BSSN) Regulation No. 8 of 2020 on Security in the Operation of Electronic Systems ("**BSSN Reg. 8/2020**")	The implementing regulation referred to in Article 24 (4) GR 71 with regard to the security system requirements on electronic system.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

Law	Sanctions
EIT Law	Administrative sanctions in the forms of: a. written warning; b. administrative fine; c. temporary suspension; and/or d. access blocking. Criminal sanction of imprisonment up to 10 years and/or criminal fine up to IDR 10billion.
GR 71	Administrative sanctions in the forms of: a. written warning; b. listed in the priority list for supervision; c. blacklisted; d. temporary suspension of services; and/or e. revocation of operating license.
BSSN Reg. 8/2020	Administrative sanctions in the forms of written warning.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

The MOCD is essentially responsible for AI-related matters.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

Indonesia has yet to introduce a law or regulation specifically on AI-related matters. However, generally, the EIT Law and its implementing regulations (GR 71, MR 20, MR 5), PDP Law and intellectual property law apply to various aspects of AI.

Several institutions have also published guidelines on the use of AI:

Soft Law	Purpose
MCIT Circular Letter No. 9 of 2023 on AI Ethics ("**CL 9**")	This guideline intended to ensure the safety of AI systems and provide legal certainty for the use in AI for business undertakings, public and private ESOs. The range of AI capabilities outlined in this circular letter includes programming that encompasses subsets such as machine learning, natural language processing, expert systems, deep learning, robotics, neural networks, and other similar technologies.
AI Code of Ethics Guidelines issued by the OJK	This guideline intended to guide financial technology providers and related parties in ensuring that AI-based applications meet the principles of being beneficial, fair and accountable, transparent and explicable, as well as robust and secure, and based on Pancasila (i.e., the Indonesian ideology).
National Strategy for AI 2020-2045 issued by the Technology Assessment and Application Agency (BPPT) which has now been integrated into the National Research and Innovation Agency (BRIN)	The document is designed to provide a mapping on the government's strategy in regulating AI.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

Indonesia has yet to introduce a law/regulation that specifically addresses the use of Large Language Models and/or generative AI. However, the soft laws under Question 21 above also covers general guidelines on natural language processing, deep learning programs, and generative AI.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

As currently there are no specific AI laws/regulations in Indonesia, no mandatory provisions that need to be inserted in the technology contracts regarding AI risk. However, the MCIT has issued Circular Letter No. 9 of 2023 on the Ethics of AI, which encourages the operator of AI to observe the safety of using AI to ensure privacy,

personal data protection, and the user's rights. In our observation, the practice to insert such AI risk provision is more common – for example inserting the limitation on AI usage in technology vendors' contract.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

As above, currently no mandatory provisions that need to be inserted in the technology contracts regarding AI risk. It is also becoming more common to insert intellectual property-related provisions in using AI – for example usage of protected intellectual property in AI systems.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

Law	Purpose
MoT Regulation No. 99 of 2018 on General Policy for Crypto Asset Futures Trading	Crypto assets defined as a commodity that can be the subject of a futures contract in a futures exchange.
Bappebti Regulation No. 2 of 2019 on the Implementation of Commodities Physical Market in Futures Exchanges, amended by Bappebti Regulation No. 10 of 2019	The mechanism for trading crypto assets in a futures exchange. It also stipulates that tradable crypto assets are those included in a list of maintained by the Head of Bappebti.
Bappebti Regulation No. 3 of 2019 on Commodities Permitted as the subject of a Futures Contract, Sharia Derivative Contract, and/or Other Derivative Contracts Traded on a Futures Exchange, as lastly amended by Bappebti Regulation No. 2 of 2025	Listing of commodities that can be the subject of a futures contract, sharia derivative contract, and/or other derivative contracts traded in a futures exchange, including crypto assets.
Bappebti Regulation No. 8 of 2021 on Guidelines for the Implementation of Physical Crypto Assets Market Trading in the Futures Exchange, as amended by Bappebti Regulation No. 13 of 2022	Guidelines for physical crypto assets market trading in futures exchanges.
Bappebti Regulation No. 11 of 2022 on the Determination of the List of Crypto Assets Traded in the Physical Crypto Assets Market, as lastly amended by Bappebti Regulation No. 1 of 2025	A list of crypto assets traded in the physical crypto assets market.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

a. Search Engines

Law	Purpose or content
EIT Law	Utilization of electronic information and transactions, including sanctions for criminal acts via the internet (propagation of defamation, hate speech, etc.).
GR 71	The implementing regulation of the EIT Law, which applies specifically to ESOs, including a prohibition on the distribution of unlawful electronic information and documents.
MR 5	Details for the takedown of unlawful content distributed via the internet and requirements to provide access to data/systems upon requested by the authority.

b. Marketplace

Law	Purpose or content
Law No. 7 of 2014 on Trading, as amended by Government Regulation In Lieu of Law No. 2 of 2022 on Job Creation, which has been ratified as a law, by Law No. 6 of 2023	General rules on trading activities, including e-commerce.
Government Regulation No. 80 of 2019 on E-Commerce	Ground rules for operations of e-commerce, including licensing, customer protection, dispute settlement, and advertising.
MoT Regulation No. 31 of 2023 on Provisions for Business Licensing, Advertising, Guidance, and Supervision of Business in Trading through Electronic System	Business licensing, advertising, guidance, and supervision of business undertakings in e-commerce.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

Law	Purpose or content
EIT Law	Utilization of electronic information and transactions, including sanctions for criminal acts via the internet (propagation of defamation, hate speech, etc.)
GR 71	Implementing regulation of the EIT Law, which specifically applies to ESOs, including a prohibition on the distribution of unlawful electronic information or document.
MR 5	Detail for the takedown of unlawful content distributed via the internet.
Government Regulation No. 17 of 2025 on Child Protection in Online System	Implementing regulation to the EIT Law, which specifically addresses compliance requirements to establish protection to child users in digital and online media, such as age limit, verification requirement, profiling, and dark patterns.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

Law	Sanctions
EIT Law	Administrative sanctions in the forms of: a. written warning; b. administrative fine; c. temporary suspension; and/or d. access blocking. Criminal sanction of imprisonment up to 10 years and/or criminal fine up to IDR 10billion.
GR 71	Administrative sanctions in the forms of: a. written warning; b. listed in the priority list for supervision; c. blacklisted; d. temporary suspension services; and/or e. revocation of operating license.
MR 5	Administrative sanctions in the form of: a. written warning; b. temporary suspension; c. access blocking; and/or d. revocation of ESO Certificate.
Government Regulation No. 17 of 2025 on Child Protection in Online System	Administrative sanctions in the forms of: a. written warning; b. administrative fine; c. temporary suspension; and/or d. access blocking.

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

Currently, there has not been any specific laws which address spatial computing. Thus, the general provisions under the EIT Law and GR 71, including their implementing regulations would apply.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

Currently, there has not been any specific laws which address quantum computing. Thus, the general provisions under the EIT Law and GR 71, including their implementing regulations would apply.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

Currently, there has not been any specific laws which address data centres. Thus, the general provisions under the EIT Law and GR 71, including their implementing regulations would apply. Additionally, certain industries (such as financial services and healthcare) are subject to sector-specific regulations that also govern the use of data centre facilities by a certain industry-specific businesses.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

a. **Privacy:** The PDP Law is effective as of October 2024. However, there has not been any significant development on the enactment of the Draft GR and the establishment of the DPA. Thus, it should be anticipated that, the government would expedite and increasing scrutiny the enforcement of the PDP Law as soon as the finalization of these pending items.
b. **Cloud Computing:** The government has issued the MOCD Regulation No. 5 of 2025 on Public Electronic Systems Operator, which expressly allows the use of third-party cloud services by public institutions. Thus, this should be viewed as a catalyst for the growth of cloud services providers and technology in Indonesia. The use of cloud services should be reasonably expected as subject to higher technology and security standards, which would encourage more industry player to develop their products in Indonesia. Ultimately, the development of cloud services would lead to the availability of more advanced and varying cloud services.
c. **Artificial Intelligence:** as AI (especially widespread use of generative AI) starts to proliferate worldwide, the Indonesian government is becoming acutely aware of the crucial need to regulate AI for everyone's benefit and protection.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Not that we are aware of. Nevertheless, it should be anticipated that the practice would be more common in the future.

As a background, Indonesia has submitted to United Nations Framework Convention on Climate Change (UNFCCC) its Long-Term Strategy for Low Carbon Resilience (LTS-LCCR) 2050, which aims to achieve Net Zero Emissions in 2060. From 2021 to 2025, the Ministry of Energy and Mineral Resources will issue a number of regulations, including on non-renewable energy (NRE), early retirement of coal-fired power plants, expansion of co-firing at coal-fired power plants, and conversion of diesel plants to running on gas and NRE power. These developments signifies the increasing in awareness of environmental sustainability by the State. Accordingly, it should be anticipated that provisions on sustainability, net-zero obligations, or similar environmental commitments would be more commonly adopted in practice.

Contributors

Agus Ahadi Deradjat
Partner
aderadjat@abnrlaw.com

Mahiswara Timur
Senior Associate
mtimur@abnrlaw.com

Dhan Kaur
Associate
dkaur@abnrlaw.com

Natasya Amalia
Associate
namalia@abnrlaw.com