COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Indonesia

TMT

Contributor

ABNR Counsellors at Law

Agus Ahadi Deradjat

Partner | aderadjat@abnrlaw.com

Kevin Sidharta

Partner | ksidharta@abnrlaw.com

Mahiswara Timur

Senior Associate | mtimur@abnrlaw.com

Nina C. Santoso

Senior Associate |

Natasya Amalia

Associate | namalia@abnrlaw.com

Vesa Puri

Associate | vpuri@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. Is there a single regulatory regime that governs software?

No. Provisions on software are broadly set out in the electronic information and transactions regulatory regime, which includes:

- Law No 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("EIT Law");
- Government Regulation No. 71 of 2019 on the Provision of Electronic Systems and Transactions ("GR 71");
- Minister of Communications and Information Technology ("MCIT") Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("MR 20");
- MCIT Regulation No. 5 of 2020 on Private Electronic Systems Operators, as amended by MCIT Regulation No. 10 of 2021 ("MR 5");
- Cyber and Crypto National Agency (BSSN) Regulation No. 8 of 2020 on Security in the Operation of Electronic Systems.

Additionally, certain aspects concerning software are also stipulated in sectoral regulations, such as: (i) Minister of Finance Regulation No. 190/PMK.04/2022 on the Release of Imported Goods for Use (procedures for software importation); and (ii) Law No. 28 of 2014 on Copyright ("Copyright Law") (software copyright protection).

2. How are proprietary rights in software and associated materials protected?

These are protected by copyright under the 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).

3. 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.

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

Yes, these are governed under the EIT Law and GR 71. The following are prohibited in relation to the operation of software/computer systems:

1. intentionally and illegally distributing or transmitting, or making accessible electronic information or documentation with content that violates decency, promotes gambling, is offensive or defamatory, or can extort/threaten people;
2. intentionally and illegally spreading false or misleading news, resulting in consumer losses in electronic transactions;
3. intentionally and illegally spreading information intended to incite hatred or hostility towards certain individuals or groups of people based on their ethnicity, religion, race, or inter-group conflict;
4. intentionally and illegally sending electronic information or electronic documentation that contains threats of violence or intimidation

aimed at people;
5. 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;
6. 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;
7. 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;
8. intentionally and illegally or unlawfully take action that disrupts an electronic system or renders an electronic system inoperable;
9. 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;
10. 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;
11. intentionally and illegally or unlawfully committing an act referred to in points (a) to (i) above that causes losses to another person;
12. 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:

1. 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;
2. to broadcast or disseminate the results of a discussion, or recording the above;
3. intentionally and illegally or unlawfully accessing the computer or electronic system of another person in any way;
4. intentionally and illegally or unlawfully accessing a computer or electronic system in any way for the purpose of obtaining electronic information or documentation;
5. intentionally and illegally or unlawfully accessing a computer or electronic system in any way by violating, bypassing, exceeding, or hacking its security system;
6. 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;
7. without permission, carrying out action that damages transmissions from programs, information, codes or orders protected by the state;
8. 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;
9. without permission, using or accessing a government-owned computer or electronic system;
10. without permission or exceeding authority, damaging a state-protected computer or electronic system;
11. without permission or exceeding authority, damaging a computer or electronic system that is dedicated for community use;
12. affecting or disrupting the operation of a government computer or electronic system;
13. 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;
14. 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;

15. 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;
16. 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;
17. 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
18. 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
19. 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.

5. To the extent not covered by (4) 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).

6. 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).

7. 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.

8. 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.

9. 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?

Currently, this is not yet the norm in Indonesia. However, this arrangement is not restricted under Indonesian laws.

10. Are there any export controls that apply to software transactions?

No, there are none.

11. 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.

12. 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.

13. Which body(ies), if any, is/are responsible for the regulation of telecommunications networks and/or services?

The main responsible authority for the regulation of telecommunications networks and services is the MCIT.

14. 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 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.
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. 12 of 2018 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.

15. Which body(ies), if any, is/are responsible for data protection regulation?

Currently, the MCIT is the responsible body for data protection. However, Law No. 27 of 2022 on Protection of Personal Data ("PDP Law") mandates the establishment of an independent Data Protection Authority ("DPA") under the supervision of the President, with extensive regulatory, monitoring, enforcement, dispute resolution, and investigative authority. To date, the DPA has yet to be established.

16. Please summarise the principal laws (present or impending), if any, that 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.

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).

17. 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).

18. 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.

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

The MCIT is essentially responsible for AI-related matters.

20. Please summarise the principal laws (present or impending), if any, that 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.

21. Are there any specific legal provisions

(present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

Indonesia has yet to introduce a law/regulation that specifically addresses the use of Large Language Models and/or generative AI.

22. Which body(ies), if any, is/are responsible for the regulation of blockchain and / or digital assets generally?

The Commodity Futures Trading Regulatory Agency ("Bappebti"), under the Ministry of Trade ("MoT"), is responsible for blockchain and digital asset-related matters.

23. 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	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 amended by Bappebti Regulation No. 4 of 2023	A list of crypto assets traded in the physical crypto assets market.

24. Are blockchain based assets such as cryptocurrency or NFTs considered "property" capable of recovery (and other remedies) if misappropriated?

Yes. Cryptocurrency is regarded as a market-tradable commodity, but NFTs are not yet specifically covered and acknowledged by Indonesian law. However, an NFT would still be considered "property" under Indonesian civil code, specifically as an intangible movable property.

Accordingly, upon a misappropriation of cryptocurrency or NFT, the interested party may seek for recovery or remedy based on the following mechanism:

- With regard to cryptocurrencies, any dispute arise between parties during operation of the Physical Crypto Assets Market, its settlement must first be aimed at through negotiation. If this is not possible, the parties may make use of facilities provided by the Future Exchange. If consensus is still not reached, the parties can settle via the Commodity Futures Trading Arbitration Board (BAKTI) or a district court.
- With regard to any dispute related to NFT, the parties may file a civil claim to the district court regarding to general dispute related to the misappropriation of NFT or to the commercial court if the dispute is related to the intellectual property aspect of the NFT.

25. Which body(ies), if any, is/are responsible for the regulation of search engines and marketplaces?

The responsible authority would be the MCIT and MoT. Particularly, the MCIT is responsible for the general operation of electronic systems (including digital platforms such as search engines and marketplace website/platform), whilst the MOT is sectoral authority responsible for the operation e-commerce businesses, including marketplace.

26. 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.

1. 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.

1. 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. 50 of 2020 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.

27. Which body(ies), if any, is/are responsible for the regulation of social media?

The responsible authority for social media would be the MCIT.

28. Please summarise the principal laws (present or impending), if any, that govern social media, 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.

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

1. Privacy: following issuance of the PDP Law in 2022, it is expected that the MCIT will publish regulations or guidelines for implementation of the PDP Law. This would help to clarify privacy compliance requirements for any party that processes personal data.
2. Cybersecurity: in light of increased data security threats, ransomware attacks and phishing, the Indonesian government is well aware of the need to strengthen security in this field.
3. Artificial Intelligence: as AI (especially widespread use of regenerative chatbots) starts to proliferate worldwide, the Indonesian government is becoming acutely aware of the crucial need to regulate AI for everyone's benefit and protection.

30. 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, its 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

Kevin Sidharta
Partner
ksidharta@abnrlaw.com

Mahiswara Timur
Senior Associate
mtimur@abnrlaw.com

Nina C. Santoso
Senior Associate

Natasya Amalia
Associate
namalia@abnrlaw.com

Vesa Puri
Associate
vpuri@abnrlaw.com