COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Indonesia

TMT

Contributor

ABNR Counsellors at Law

Agung Ahadi Deradjat

Partner | aderadjat@abnrlaw.com

Kevin Sidharta

Partner | ksidharta@abnrlaw.com

Mahiswara Timur

Senior Associate | mtimur@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. Are communications networks or services regulated?

Yes. The telecommunications industry is regulated by Law No. 36 of 1999 on Telecommunications, as amended by Law No. 11 of 2020 on Job Creation ("**Telecommunications Law**") and its implementing regulations, which include:

- Government Regulation No. 52 of 2000 on the Implementation of Telecommunications, as 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;
- Ministry of Communications and Information Technology ("**MCIT**") Regulation No. 01/PER/M.KOMINFO/01/2010 on Implementation of Telecommunications Networks, as amended and partially revoked several times, last by MCIT Regulation No. 5 of 2021 on the Implementation of Telecommunications ("**MR 01/2010**");
- MCIT Regulation No. 12 of 2018 on Provision of Special Telecommunications for the Needs of Government Agencies or Legal Entities ("**MR 12/2018**");
- MCIT Regulation No. 13 of 2019 on the Implementation of Telecommunications Services, as amended several times, last by MCIT Regulation No. 14 of 2021;
- MCIT Regulation No. 5 of 2021 on the Implementation of Telecommunications ("**MR 5/2021**"), (collectively referred to as "**Telco Regulations**").

2. If so, what activities are covered and what licences or authorisations are required?

In general, telecommunications operation is classified as:

(a) Operation of telecommunications networks:

- Fixed networks
    - Fixed local;
    - Fixed long-distance connections;
    - Fixed international connections;
    - Fixed closed networks; and
    - Others as stipulated by the MCIT.
- Mobile networks
    - Terrestrial mobile;
    - Cellular mobile;
    - Satellite mobile; and
    - Others as stipulated by the MCIT.

(b) Operation of telecommunications services

- Basic telephony services
    - Telephone;
    - Facsimile;
    - Short Messaging Services ("SMS"); and/or
    - Multimedia Messaging Services (MMS).
- Value-added telephony services
    - Call Centre Information;
    - Calling Cards;
    - Internet Telephony for Public Purposes;
    - Premium Calling;
    - Premium SMS Content; and/or
    - Other Value-Added Telephony.
- Multimedia services
    - Internet Provision;
    - Network Access Points ;
    - Data Communications Systems;
    - Internet Protocol TV; and/or
    - Other Multimedia Services.

(c) Operation of special telecommunication services

Special telecommunications operations are telecommunications operations with special characteristics, designations, and operations for use by government agencies or legal entities.

The operation of special telecommunications may

transmit via:

- wire;
- optical fiber;
- radio frequency spectrum; and/or
- other electromagnetic systems.

In addition to general licensing and registration, the operation of a telecommunications network/service requires a specific telecommunications license from the MCIT for the corresponding telecommunication service or networks (cited above). In, addition approval or a permit might be required for certain telecommunications operations, such as for the use of radio frequency, satellite, or subsea cables.

3. Is there any specific regulator for the provisions of communications-related services?

Yes, the main regulator for telecommunications operation is the MCIT.

4. Are they independent of the government control?

The MCIT is a government agency, reporting to the President.

5. Are platform providers (social media, content sharing, information search engines) regulated?

Yes, platform providers are regulated under a different regime: Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 ("**EIT Law**") and its implementing regulations:

- Government Regulation No. 71 of 2019 on the Provision of Electronic Systems and Transactions ("**GR 71/2019**");
- MCIT Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems ("**MR 20/2016**");
- MCIT Regulation No. 5 of 2020 on Private Electronic Systems Operators, as amended by MCIT Regulation No. 10 of 2021;
- Government Regulation No. 80 of 2019 on E-Commerce; and
- Minister of Trade ("**MOT**") Regulation No. 50 of 2020 on the Provision of Business Licensing, Advertising, Management, and Supervision of E-Commerce Undertakings ("**MR 50/2020**").

However, several provisions under the Telco Regulations concern platform providers, such as an obligation for internet business undertakings that meet certain thresholds to cooperate with Indonesian telecommunications operators.

6. If so, does the reach of the regulator extend outside your jurisdiction?

The Telco Regulations are limited in reach and do not extend beyond Indonesia.

However, the EIT Law and its implementing regulations apply extraterritorially. However, practical enforcement of the law on offshore entities is rather limited, as Indonesian authorities would require cooperation from international authorities and the offshore entities themselves.

7. Does a telecoms operator need to be domiciled in the country?

Yes, telecommunications network/services operators must be domiciled in Indonesia. Pursuant to MR 5/2021, operation of a telecommunications network and services can only be performed by: (i) state-owned enterprises; (ii) regional government-owned enterprises; (iii) private legal entities; and (iv) cooperatives.

8. Are there any restrictions on foreign ownership of telecoms operators?

No, telecommunications network/services operation is 100% open to foreign ownership.

9. Are there any regulations covering interconnection between operators?

Yes, interconnection (connectivity between telecommunications networks from different telecommunications network operators) is covered under the Telco Regulations.

MR 5/2021 stipulates that interconnection must be provided by a telecommunications network operator based on demand from other telecommunications network operators, in a transparent and non-discriminatory manner (including interconnection fees charged by a destination operator to an origin operator).

It is worth noting that under certain conditions interconnection is prohibited, such as between fixed-closed network operators and special

telecommunications operators, as stipulated in MR 01/2010 and MR 12/2018.

10. If so are these different for operators with market power?

Yes, MR 5/2021 requires that the Director General of Posts and Informatics ("**DGPI**") identify Telecommunications Operators that provide interconnection services with a dominant position or a deemed dominant position that control: (i) 50% or more; or (ii) the largest share of operating revenue of the total operating revenue of all Telecommunications Network operations providing basic telephony services.

In this instance, Telecommunications Network Operators with a dominant position would be subject to more exhaustive evaluation by the DGPI if amending their Interconnection Offering Document (DPI).

MR 5/2021 further prohibits telecommunications network operators from carrying out discriminatory practices in the provision of interconnection. In addition, a general prohibition is imposed on telecommunications network and services operators from implementing tariffs that interfere with consumer protection, fair business competition, or continuity of service to the public.

11. What are the principal consumer protection regulations that apply specifically to telecoms services?

In addition to the general consumer protection obligations under Law No. 8 of 1999 on Consumer Protection, telecoms services are subject to specific consumer protection requirements under the Telco Regulations. MR 5/2021 stipulates that telecommunications network and services operators are prohibited from implementing tariffs that interfere with consumer protection, fair business competition, or continuity of service to the public. The prohibition from engaging in discriminatory practices is also aimed at protecting consumers.

The DGPI oversees the supervision and controls the implementation of network lease services and application of tariffs by telecommunication network and service operators for this purpose.

12. What legal protections are offered in relation to the creators of computer software?

The legal protection offered in relation to the creators of computer software is copyright under Law No. 28 of 2014 on Copyright ("**Copyright Law**"). Computer software herein is deemed a computer program (a set of instructions expressed in the form of language, code, schematics, or another form intended to make a computer work to perform a certain function or achieve a certain result). The creators are afforded with automatic copyright protection for 50 years as of the first announcement, as registration is not a pre-requisite to copyright protection.

13. Do you recognise specific intellectual property rights in respect of data/databases?

Protection of data/databases could be afforded under the Copyright Law. Under the law, a copyrighted Creation may be in the fields of science, art, and literature, including: (i) a database (compilation of data in any form that can be read by a computer, or a compilation in any other form); (ii) compilation of a Creation or data, whether in a format that can be read by a computer program or other media. Protection of the database is provided without prejudice to the rights of the authors of the Creation entered in the database.

14. What key protections exist for personal data?

Personal data protection is regulated under the EIT Law and its implementing regulations, which includes the following key requirements:

- mandatory express consent requirement for personal data processing;
- an obligation to safeguard the confidentiality of personal data;
- an obligation to encrypt stored personal data;
- an obligation to report data breaches to law enforcement authorities and relevant ministries/institutions, and notify the data subjects concerned;
- imposition of criminal and administrative sanctions for any violation related to personal data protection laws and regulations, including unauthorized access, disclosure, and wiretapping.

15. Are there restrictions on the transfer of personal data overseas?

Pursuant to MR 20/2016, transfer of personal data managed by an Electronic Systems Operator (ESO) domiciled in Indonesia to an offshore location must:

- be coordinated with the MCIT or an authorized official/agency (currently carried out by way of submitting an annual report to the MCIT); and
- comply with the sectoral laws and regulations on cross-border personal data transfer (e.g., in e-commerce sector, personal data can only be transferred to countries or regions that have been"white-listed" by the Ministry of Trade, for maintaining equal protection standards and levels with Indonesia).

16. What is the maximum fine that can be applied for breach of data protection laws?

The current regulation does not stipulate the amount of possible administrative fine that may be imposed on ESOs for breach of data protection laws. Further, the government is currently drafting a regulation on Types and Tariffs for Non-Tax State Revenues Applicable at the MCIT, including for non-compliance by ESOs in the private sector ("**Private ESOs**") with obligations on the operation of electronic systems.

In the absence of a written regulation, it is likely that the MCIT would not impose a fine for non-compliance. On the downside, it would be more likely that the MCIT would immediately block access.

17. What additional protections have been implemented, over and above the GDPR requirements?

The current Indonesian data protection laws and regulations do not contain additional protection over and above the GDPR requirements, as GDPR generally does not apply in Indonesia. However, Indonesian data protection law provides protection of the processing of personal data via electronic means. This includes:

- Mandatory consent for processing personal data, on all occasions;
- The minimum retention period of personal data is 5 years, unless stipulated otherwise;
- In the event of a failure or disturbance that has a serious impact as a result of action of another party on an electronic system, an ESO must immediately report it at the first opportunity to MCIT and the data subject concerned; and
- Indonesian data protection regulations have yet to differentiate between processors and controllers.

Furthermore, the Government is preparing a bill on personal data protection ("PDP Bill"), which is designed to adopt the GDPR principles. However, it is unclear when the PDP Bill will be issued and promulgated as law.

18. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

No specific regulation exists for cloud-based services. However, they would be subject to the EIT Law and its implementing regulations, as well as the e-commerce regulations (if provided commercially). The provision of these services would constitute operation of an electronic system under GR 71/2019, and the ESO operating/providing the services must comply with licensing (for onshore ESOs), registration (for both onshore and offshore ESOs), and data protection requirements under these regulations.

19. Are there specific requirements for the validity of an electronic signature?

Yes. Pursuant to the EIT Law and GR 71/2019, an electronic signature ("**E-Signature**") will only be legally valid and have legal effect if it fulfils the following criteria:

- the personal, biometric, or cryptographic code, or the code yielded from the conversion of a manual signature into an E-Signature, including other codes resulting from the development of Information Technology (**Creation Data**), must be associated only with the signatory;
- during the electronic signing process, the Creation Data must be in the sole possession of the signatory;
- alterations to the E-Signature, after signing, are clearly accessible;
- alterations to the electronic information associated with the E-Signature after signing are clearly accessible;
- a specific method is adopted to identify the signatory; and
- there is a specific method to demonstrate that the signatory has given consent to the related electronic information in the document.

According to GR 71/2019, E-Signatures are classified as:

(1) **Certified E-Signatures:** which are made using an electronic certificate issued by an Indonesian Electronic Certification Authority (CA); and

(2) **Non-Certified E-Signatures:** which are made without involving an Indonesian CA.

The significant difference between Certified and Non-Certified E-Signatures lies in their evidentiary value when presented before an Indonesian court, in which *Non-Certified E-Signatures are considered to possess less evidentiary value than Certified E-Signatures.*

20. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

No. A contract-based outsourcing supplier would only provide services to the procuring entity based on the outsourcing agreement; thus, there would not be automatic transfer of employees, assets, or third-party contracts of the procuring entity to the outsourcing supplier. These would remain with the procuring entity.

21. If a software program which purports to be a form of A.I. malfunctions, who is liable?

We view that 3 parties exist in this scenario: the program developer, the program operator, and the user. Criminal and administrative liabilities in the applicable laws and regulations would most likely be imposed on the program operator, unless gross negligence or bad faith is attributable to the program developer.

As regards civil claims, users would most likely file these against the program operator. The program developer would likely be liable for civil claims filed by the program operator.

22. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

(a) obligations as to the maintenance of cybersecurity; and

Cybersecurity is generally regulated under the EIT Law and its implementing regulations. Under the EIT Law, ESOs are required to provide electronic systems in a reliable and secure manner and take responsibility for the proper operation of electronic systems. This security covers the protection of electronic systems, including the security hardware and software.

Further, GR 71/2019 requires ESOs to maintain security measures and systems in order to avoid interference, failure, and loss relating to electronic systems, including procedures and systems for prevention and response to threats and attacks that cause disturbances, failures, and losses (such as antivirus, anti-spamming, firewall, intrusion detection, prevention system, and/or management of information security management systems). However, the regulations are silent as to specific prevention and mitigation procedure and systems that must be implemented.

Nonetheless, there are sectoral cybersecurity requirements that apply to specific industries such as banking, financial services, e-commerce, telecommunications, and health. These sectoral regulations generally require service providers to ensure confidentiality of information and data, unless explicitly exempted (e.g., for law enforcement purposes).

(b) the criminality of hacking/DDOS attacks?

The key law regulating cybercrime is the EIT Law. Hacking/DDOS attacks would be deemed illegal access under Article 30 of the EIT Law (intentional and unauthorized or unlawful access to a computer or electronic system belonging to another person, in order to obtain information by breaching, hacking, trespassing, or breaking through security systems), which is subject to criminal sanction of imprisonment (up to 8 years) or a fine (up to IDR 800 million).

23. What technology development will create the most legal change in your jurisdiction?

In view of the lack of legal framework on artificial intelligence (AI), particularly in relation to use of algorithms, the development of this technology would create a significant legal change in Indonesia. The Government would face challenges as to how AI could be limited and controlled within the Indonesian environment, including the legal liability aspects of AI operation.

We also view that the rapid growth of cloud services that allow the provision of services: (i) which may substitute conventional services previously regulated; and (i) virtually from anywhere around the world, could pose a challenge to the Indonesian legal system. The strict and conservative nature of Indonesian regulations may not accommodate the evolution of cloud-based services, resulting in a regulatory gap. This is especially challenging for regulators in highly controlled sectors (finance and banking).

24. Which current legal provision/regime

creates the greatest impediment to economic development/ commerce?

In the data protection sector, we have seen that foreign businesses are particularly concerned with: (i) mandatory ESO registration; (ii) a requirement to comply with takedown requests from the MCIT within relatively short turnaround times, as well as (iii) authority overreach in requesting access to electronic information/systems (which may be at odds with compliance with law and regulations in other jurisdictions).

In e-commerce, the threshold that triggers a requirement for foreign e-commerce undertakings to establish a representative office in Indonesia is relatively low (more than 1,000 transactions/1,000 packages delivered within a year), potentially resulting in the requirement being applicable to all foreign businesses planning to enter the Indonesian market.

Finally, we also view that strict and extensive requirements under telecommunications regulations may, in essence, limit the development of telecommunications in Indonesia.

25. Do you believe your legal system specifically encourages or hinders digital services?

On one side, certain regulations under Indonesian law encourage digital services. For example, the EIT Law adopts the principle of technology neutrality, which theoretically allows the introduction of new technologies. However, particularly during practical implementation of the regulations, the Government tends to adopt an overcautious approach, which often disregards technological aspects and the inherently/inevitable cross-border nature of the digital industry, which can hinder the development of digital services.

26. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

We view that our current legal system is not yet ready to deal with the legal issues associated with AI. There is currently neither an adequate regulatory framework nor instruments (in a practical sense) to address the issues, so legal development is falling short compared with technological development.

Contributors

Agung Ahadi Deradjat
Partner
aderadjat@abnrlaw.com

Kevin Sidharta
Partner
ksidharta@abnrlaw.com

Mahiswara Timur
Senior Associate
mtimur@abnrlaw.com