

Country Comparative Legal Guides

Indonesia: Technology

Country Author: [SSEK Legal Consultants](#)



Fahrul S. Yusuf,
partner

fahrulyusuf@ssek.com

This country-specific Q&A provides an overview to technology laws and regulations that may occur in [Indonesia](#).

It will cover communications networks and their operators, databases and software, data protection, AI, cybersecurity as well as the author's view on planned future reforms of the merger control regime.

This Q&A is part of the global guide to Technology. For a full list of jurisdictional Q&As visit <http://www.inhouselawyer.co.uk/index.php/practice-areas/technology>

1. Are communications networks or services regulated? If so what activities are covered and what licences or authorisations are required?

Yes, communications networks and services are regulated in Indonesia. Law No. 36 of 1999 regarding Telecommunications (September 8, 1999) divides telecommunications operations into three areas:

a. telecommunications networks:

1. Fixed-line networks consisting of local, domestic long-distance, international and closed fixed networks; and
2. Mobile networks consisting of mobile terrestrial networks, mobile cellular networks and mobile satellite networks.

b. telecommunications services:

1. Basic telephone services using circuit switched technology or other technology to provide telephone, facsimile, telex, telegraph and data transmission services;
2. Value-added telephone services including premium calls, calling cards, virtual private phone numbers, store and forward, and call centres; and
3. Multimedia services including internet service providers, network access points, internet telephony (VOIP), and data communication system services.

c. special telecommunications for individual purposes, security and defence.

The license required would ultimately depend on which field of telecommunication is being conducted by the business entity. Generally, the license or approval to engage in the telecommunication business will have to be obtained from the Ministry of Communication and Informatics ("MOCI") or one of its Directorates General.

2. Is there any specific regulator for the provisions of communications-related services? Are they independent of the government control?

In Indonesia, the regulator for the provision of communications-related services is the MOCI and the Directorate General of Post and Telecommunication ("DGPT").

Aside from the MOCI and DGPT, there is also the Indonesian Telecommunication Regulatory Body (Badan Regulasi Telekomunikasi Indonesia), which consists of the DGPT and the Telecommunication Regulation Committee. These regulators are not independent of government control.

3. Does an operator need to be domiciled in the country? Are there any restrictions on foreign ownership of telecoms operators?

Yes, telecoms operators need to be in the form of an entity domiciled in Indonesia in order to conduct business. There is a foreign ownership restriction of 67% for telecoms operators, i.e.:

1. fixed telecommunication network provider;
2. moving telecommunication network provider;
3. service-integrated telecommunication network provider;
4. telecommunication content service provider;
5. information service (call centre) and other value-added telephone service provider;
6. internet service provider;
7. data communication system provider;
8. internet telephone provider (for public purposes); and
9. internet interconnection services (NAP) and other multimedia services.

4. Are there any regulations covering interconnection between operators? If so are these different for operators with market power? What are the principal consumer protection regulations that apply specifically to telecoms services?

Interconnection between operators is regulated under MOCI Regulation No. 09/Per/M.KOMINF/02/2006 regarding Interconnection (February 8, 2006). There are no other regulations specifically regulating operators with market power.

Aside from Law No. 8 of 1999 regarding Consumer Protection (April 20, 1999), which provides the general framework for consumer protection, there are no consumer protection regulations that apply specifically to telecoms services.

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

The legal protections offered creators of computer software are those in relation to intellectual property. Under Law No. 28 of 2014 regarding Copyright (October 16, 2014), computer programs (inclusive of software) are granted the same type of protections as more conventional creations (e.g., books, art, music). These protections include imprisonment and/or fines in varying lengths and amounts, depending on the severity of the violation, for any violation of a copyright holder's economic rights.

6. Are specific intellectual property rights in respect of data/databases recognised?

No specific intellectual property rights exist under Indonesian law in respect of data/databases.

7. What key protections exist for personal data?

The key protections for personal data under Indonesian law are:

1. the requirement of consent for any electronic system provider to handle personal data (e.g., collecting, processing, distributing);
2. the requirement of data-onshoring for any electronic system provider providing "public services" (as explained below);
3. the requirement of full disclosure for any use of personal data;
4. the deletion of personal data after a certain period of time or at the request of the personal data owner.

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

Yes. Under MOCI Regulation No. 20 of 2016 regarding Protection of Personal Data in Electronic Systems (December 1, 2016) ("MOCI Reg"), the transfer of personal data overseas requires the local transferor to satisfy a coordination requirement with the

MOCI and to fulfil any regulatory provision regarding the cross-border transfer of personal data (i.e., consent). The coordination requirement consists of:

1. reporting any plan to transfer personal data, which must contain at least the clear name of the receiving country, the full name of the receiver, date of implementation, and reason/purpose of the transfer;
2. requesting advocacy, if necessary; and
3. reporting the result of the transfer.

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

The maximum fine that can be applied for breach of data protection laws is contained in Law No. 11 of 2008 regarding Electronic Information and Transactions (April 21, 2008), as amended (“ITE Law, as amended”), namely IDR12 billion (approximately USD900,000 at current conversion rates).

10. Are there any restrictions applicable to cloud-based services?

A possible restriction imposed on cloud-based services is data-onshoring (i.e., having a local data centre and disaster recovery centre). This requirement is contained in Government Regulation No. 82 of 2012 regarding Provision of Electronic Systems and Transactions (October 15, 2012) (“GR 82/2012”) and its implementing regulation on electronic system providers that conduct a “public service.” “Public service” is defined as an “an activity or series of activities in the fulfilment of the need for services in accordance with laws and regulations for every citizen and resident toward the goods, services, and/or the administrative services provided by the public service provider.”

The plain understanding of “public service” makes it unlikely that the data-onshoring requirement would be imposed on cloud-based services. However, in practice, all local electronic service providers are obliged by the institution issuing their license to establish a data centre in Indonesia.

Other than data-onshoring, Indonesian law provides various guidelines on such matters as registration, hardware, software (which is only pertinent for an electronic

system provider for public service, aside from the general obligation to ensure the secrecy of the source code of the software used), expert workforce, electronic system management procedures, security measures, electronic system feasibility certificate, and supervision.

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

Under the ITE Law, as amended and GR 82/2012, the following are the minimum validity requirements for an electronic signature:

1. the data creation of the electronic signature is relevant to the signatory;
2. the data creation of the electronic signature during the signing is only within the possession of the signatory;
3. all changes to the electronic signature that occur after signing can be known;
4. all changes to electronic information related to the electronic signature after signing can be known;
5. there are certain methods used to identify the signatory; and
6. there are certain methods to show that the signatory has given consent for the relevant electronic information.

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

No. The employees, assets or third-party contracts remain with the outsourcing company unless otherwise regulated under the outsourcing contract or transferred under a separate transaction.

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

As Indonesian law has yet to regulate artificial intelligence ("A.I."), reference must be made to Law No. 8 of 1999 regarding Consumer Protection (April 20, 1999) (the

“Consumer Protection Law”). Under the Consumer Protection Law, an entrepreneur shall be liable for any damages sustained by the consumer due to the goods and/or services produced or traded by such entrepreneur. As such, in the event of an A.I. malfunction, the entrepreneur shall be liable for all damages suffered by the consumer of such A.I.

14. What key laws exist in terms of obligations as to the maintenance of cybersecurity?

Cybersecurity maintenance obligations are not contained in one specific regulation. Instead, they are scattered within several regulations, namely:

1. ITE Law, as amended;
2. GR 82/2012; and
3. MOCI Reg.

15. What key laws exist in terms of the criminality of hacking/DDOS attacks?

Indonesian law does not have any specific regulation on hacking/DDOS attacks. Instead, such actions are covered under the broad scope of the ITE Law, as amended and its implementing regulations.

Firstly, the ITE Law, as amended covers hacking through a prohibition for any person to purposefully, illegally, and without any rights:

1. access another person’s computer and/or electronic system using any method;
2. access a computer and/or electronic system using any method in order to obtain electronic information and/or electronic documents;
3. access a computer and/or electronic system using any method by violating, trespassing, surpassing, or penetrating the security system.

The conduct of the above actions is subject to imprisonment of six to eight years and/or fines of IDR600 million to IDR800 million (approximately USD45,000 to USD60,000 at current exchange rates).

There is no tailored provision in the ITE Law for DDOS attacks. Instead, it falls under the general prohibition on “causing disruption of an electronic system and/or causing an electronic system not to function as it should.” The failure to abide by such prohibition is subject to maximum imprisonment of 10 years and/or a maximum penalty of IDR10 billion (approximately USD750,000 at current exchange rates).

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

One of the newest technology developments that has kick-started a progression of changes in many areas of Indonesian law is the emergence of application-based transportation services, e.g., Uber, Grab, and Go-Jek. Previously, a line divided the transportation business and the application provider business, in that a company could not “provide transportation” when it was “only” supported by a mobile application, with no actual fleet of vehicles by its side. The appearance of application-based transportation services triggered the issuance and amendment of various regulations, including the amendment of the Business Fields Standard Classification (Klasifikasi Baku Lapangan Usaha Indonesia or “KBLI”) and the issuance of a Ministry of Transportation regulation that specifically regulates the provision of non-trajectory public transport, to name a few.

17. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

While the impediment is not great, the data-onshoring requirement as contained in GR 82/2012 and its implementing regulations poses an obstacle to foreign investment. Due to the broad wording of “public services,” as explained above, potential foreign investors, especially those handling data and its processing, tread lightly in investing in Indonesia. In our experience, foreign investors prefer to keep and maintain their data outside of Indonesia, particularly in countries that are renowned for their advanced and more detailed data protection regulations or in countries where the investors already have a data centre set up and running. While for major players the data-onshoring requirement may seem like a small sacrifice for the investment returns, to newer players in the market with less capital, the data-onshoring requirement may be the tipping point that drives their business away from Indonesia.

18. Do you believe the legal system specifically encourages or hinders digital services?

We view that the Indonesian legal system is trying to simultaneously encourage digital services while providing adequate security regulation for citizens' personal data. In principle, through this balance, users of digital services will be more comfortable using such digital services, knowing that their data is sufficiently protected by the law. An increased demand for digital services, in turn, should boost the digital services business in Indonesia by local and foreign investors attracted by the large market.

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

As discussed above, Indonesian does not as yet have any specific regulation for artificial intelligence; there is only the general Consumer Protection Law. We believe that more specific, advanced regulations concerning A.I. (e.g., whether A.I. can, on its own, be considered a legal subject equivalent to individuals and entities; what rights and obligations must be conferred upon an A.I.) must be issued by the Indonesian government to fully deal with the legal issues associated with A.I.