COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

Indonesia

TECHNOLOGY

Contributing firm

SSEK Legal Consultants

Fahrul S. Yusuf

Partner | fahrulyusuf@ssek.com

Albertus Jonathan Sukardi

Associate | albertussukardi@ssek.com

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

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

INDONESIA
TECHNOLOGY

1. What is the regulatory regime for technology?

The term "technology" covers a broad range of topics in various fields, each with its own laws, regulations and implementing policies, as well as principal regulator. The current regulatory regime in Indonesia covers, among other things, e-commerce, financial technology (fintech), telecommunications, cryptocurrencies, electronic information and transactions, media and entertainment, intellectual property, artificial intelligence, and related aspects of internet usage. Indonesia is a civil law jurisdiction that does not follow court precedent in formulating laws. The Government has enacted specific laws for different areas of the technological sector, and the relevant ministries and institutions have subsequently issued implementing regulations and/or policies to further implement these laws.

The main laws governing technology in Indonesia include the following:

- Law Number 11 of 2008, as amended by Law No. 19 of 2016 on Electronic Information and Transactions ("**EIT Law**");
- Law No. 36 of 1999 on Telecommunications, as amended by Law No. 11 of 2020 on Job Creation ("**Telecom Law**");
- Law No. 32 of 2002 on Broadcasting, as amended by Law No. 11 of 2020 on Job Creation ("**Broadcasting Law**");
- Law No. 13 of 2016 on Patents, as amended by Law No. 11 of 2020 on Job Creation ("**Patent Law**");
- Law No. 28 of 2014 regarding Copyright ("**Copyright Law**");
- Law No. 20 of 2016 on Trademark and Geographical Indications, as amended by Law No. 11 of 2020 on Job Creation ("**Trademark Law**");
- Law No. 8 of 1999 on Consumer Protection;
- Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions ("**GR 71/2019**");
- Minister of Communication and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems ("**MOCI Reg. 20/2016**");
- Minister of Communication and Informatics Regulation No. 5 of 2020 on Private-Scope Electronic System Providers, as amended by Minister of Communication and Informatics Regulation No. 10 of 2021 ("**MOCI Reg. 5/2020**"); and
- Ministry of Trade Regulation No. 50 of 2020 on Business Licensing, Advertisements, Guidance and Supervision of Business Actors in Trading Through Electronic Systems ("**MOT Reg. 50/2020**").

Depending on the field of technology, the relevant regulations and their derivative regulations may differ from one another. For instance, general matters concerning telecommunications, electronic information and transactions, and online sites will be regulated primarily by the Telecom Law and the EIT Law, and their derivative regulations such as Government Regulations and regulations of the Ministry of Communication and Informatics ("**MOCI**"). Cryptocurrencies are regulated by a specific body under the auspices of the Ministry of Trade ("**MOT**"), called the Futures Commodity Trading Supervisory Body (*Badan Pengawas Perdagangan Berjangka Komoditi* or "**Bappebti**"). Bappebti regulations are formulated based on the principles of the EIT Law. Financial technologies such as online lending platforms, e-money, e-wallets, payment processors, etc. are regulated and supervised by both the Indonesian Financial Services Authority (*Otoritas Jasa Keuangan* or "**OJK**") and the Indonesian Central Bank (Bank Indonesia or "**BI**").

It is also important to note that the Indonesian government has enacted Law No. 11 of 2020 on Job Creation, which introduced changes to laws on technology. It also enacted Presidential Regulation No. 10 of 2021, as amended by Presidential Regulation No. 49 of 2021, regarding Investment Sectors. This 2021 Presidential Regulation governs new foreign

shareholding limitations for several business fields related to technology.

2. Are communications networks or services regulated?

Communication networks and services are regulated mainly under the Telecom Law. The principal regulator is the MOCI. Under the auspices of the MOCI are several sub-level regulators, including the Directorate General of Post and Informatics ("**DGPPI**"). Aside from the Telecom Law, there are other relevant regulations that govern communication networks and services. Some of these were issued as implementing regulations for the Telecom Law and others are just related to it, as follows:

- the EIT Law;
- Government Regulation No. 52 of 2000 on Telecommunications Operation, as amended by Government Regulation No. 46 of 2021 on Post, Telecommunications, and Broadcasting;
- Government Regulation No. 53 of 2000 on the Utilisation of Radio Frequency Spectrum and Satellite Orbit, as amended by Government Regulation No. 46 of 2021 on Post, Telecommunications, and Broadcasting;
- GR 71/2019;
- Government Regulation No. 5 of 2021 on the Implementation of Risk-Based Business Licensing;
- MOCI Regulation No. 5 of 2021 regarding Telecommunications Operation;
- MOCI Regulation No. 1 of 2010 regarding Telecommunications Network Operation, as last amended by MOCI Regulation No. 5 of 2021 regarding Telecommunications Operation;
- MOCI Reg. 20/2016;
- MOCI Regulation No. 7 of 2018**,** as last amended by MOCI Regulation No. 5 of 2021 regarding Telecommunications Operation;
- MOCI Regulation No. 13 of 2019, as last amended by MOCI Regulation No. 1 of 2021 regarding Telecommunication Services Operations;
- MOCI Regulation No. 5 of 2020, as last amended by MOCI Regulation No. 10 of 2021 regarding Private-Scope Electronic System Providers; and
- MOCI Circular Letter No. 3 of 2016 on the Provision of Applications and/or Content Services through the Internet (Over the Top).

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

The Telecom Law divides telecommunications operations into three areas, namely:

a) Telecommunication networks

1. Fixed-line networks, consisting of fixed local networks, fixed long-distance networks, fixed international networks, fixed closed networks and other types of fixed-line networks set forth by the MOCI.
2. Mobile networks, consisting of mobile terrestrial networks, mobile cellular networks, mobile satellite networks and other types of mobile networks set forth by the MOCI.

b) Telecommunication services

1. Basic telephone services, provided by circuit switched-based local permanent network operators, long-distance direct connection permanent network operators, international direct connection permanent network operators, mobile cellular network operators, mobile satellite network operators and terrestrial mobile network operators.
2. Value-added telephone services, including telephony internet services for public needs, call centre services, premium short message services and calling card services.
3. Multimedia services, including internet service providers, network access points, internet telephony (VOIP) and data communication system services.

c) Special telecommunication operations

1. Special telecommunications for individual/internal use.
2. Special telecommunications for national defence, navigation and other governmental-specific purposes.
3. Broadcasting.

The license required will depend on the field of telecommunication services or operations in which the business entity is going to engage. Generally, the license or approval will be obtained from the MOCI, DGPPI, or another directorate under the MOCI.

Following the Job Creation Law's amendment of the Telecom Law, the licensing and authorization to engage in the abovementioned telecommunication business activities is obtained from the central government in the

form of a business license, through the Online Single Submission (OSS) system, Indonesia's principal electronic business licensing system.

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

In Indonesia, the Ministry of Communication and Informatics (MOCI) is authorized to regulate the provision of communications-related services. The DGPPI and the other directorates general under the MOCI primarily supervise and regulate telecommunications-related services, electronic platform usage, etc.

There was previously a separate regulatory body, called the Indonesian Telecommunications Regulatory Authority (*Badan Regulasi Telekomunikasi Indonesia* or "**BRTI**"). BRTI was dissolved in November 2020 and its authority subsumed by the MOCI through Presidential Regulation No. 112 of 2020.

5. Are they independent of the government control?

No, the regulator is not independent of government control. The MOCI itself is a ministry that answers directly to the president.

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

Platform providers involving social media and content sharing, including user-generated content, and information search engines are regulated under MOCI Reg. 5/2020. Under this regulation, both domestic and foreign platform providers must register with the MOCI through the OSS system prior to the operation of the platform for users. After registration, platform providers will receive a Registration Certificate issued by the MOCI. Failure to comply with the registration requirement will result in access blocking by the Indonesian government. The government also may block access to a platform if the provider neglects its obligation to take down any content, information, or document that violates the law and disturbs public order.

Furthermore, platform providers that specifically provide their platform for e-commerce (where users may purchase and sell goods and/or services) must also comply with MOT Reg. 50/2020. By virtue of this regulation, platform providers are required to have a Trade Business License through Electronic System (*Surat Izin Usaha Perdagangan melalui Sistem Elektronik* or "**SIUPMSE**") to carry out their business. Foreign e-commerce platform providers that meet certain transaction threshold (i.e., more than 1,000 sales in a year or more than 1,000 shipments to Indonesian customers) also are obligated to appoint a local representative office in Indonesia, apply for a business license and register as an ESP.

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

Article 2 of the EIT Law (and therefore its implementing regulations) purports to have extraterritorial applicability, extending the reach of the regulator beyond the borders of Indonesia, in particular for websites, applications, and electronic platforms. Generally, we note that the extraterritorial enforcement of the EIT laws, particularly against foreign entities, is lacking in practice and we are not aware of the Indonesian government enforcing the extraterritorial application. We note, however, that the enactment of MOCI Reg. 5/2020 indicates a more progressive approach by the Government toward enforcing certain terms on foreign ESPs, in particular ESP registration.

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

Yes, telecoms operators are required to be established in the form of an entity domiciled in Indonesia, pursuant to the Telecom Law. The MOCI only accepts telecommunication business license applications from Indonesian legal entities.

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

By virtue of the enactment of Presidential Regulation No. 10 of 2021 regarding Investment Sectors, the previously applicable foreign ownership cap of 67% for telecom operators has been revoked. Foreign investment companies are now allowed to have 100% ownership of telecoms operators.

10. Are there any regulations covering interconnection between operators?

Interconnection between operators is regulated under MOCI Regulation No 5 of 2021 regarding Telecommunications Operation. Under this regulation, interconnection between telecommunications operators

must be conducted in a transparent and non-discriminatory manner, based on an agreed fee.

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

No, the regulations do not differentiate between operators with market power and those without.

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

There are no consumer protection regulations that specifically govern telecoms services. Consumer protection generally with respect to any commercialization of goods and services is regulated under Law No. 8 of 1999 on Consumer Protection.

The general obligations under the Consumer Protection Law include to act in good faith in conducting business; provide correct, clear and honest information regarding the condition of and guarantees for goods and/or services; and provide clear information on the use, repair and maintenance of goods and/or services. Obligations also include to treat and serve consumers properly, honestly and without discrimination; guarantee the quality of goods and/or services produced and/or traded based on the applicable provisions on the applicable quality standards; give consumers the opportunity to test and/or try certain goods and/or services, and provide a guarantee and/or warranty for goods that are produced and/or traded; provide compensation, indemnity or replacement for losses due to the consumption of goods and/or services; and to provide compensation, indemnity and/or replacement if the goods and/or services received are not in accordance with the agreement. There also are prohibitions under the Consumer Protection Law on mislreading or misrepresenting advertisements with respect to the quality and price of goods or services.

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

Creators of computer software are legally protected by the Copyright Law. Under this law, computer software is granted the same protection as more conventional artistic creations such as books and art. Copyright protection for computer software arises automatically by law, without requiring the registration of the software with a government body. Legal protections include imprisonment and/or fines of varying lengths and amounts for copyright violators, depending on the severity of the violation of a copyright holder's economic and/or moral rights.

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

The Copyright Law explicitly defines "database" as a creation that is subject to copyright protection. Pursuant to the Copyright Law's elucidation, "database" may comprise any data compilation in any format which is readable by computer or any other compilation, which due to selection or configuration of such data becomes an intellectual creation.

15. What key protections exist for personal data?

Currently, key protections for the processing and usage of personal data exist under the EIT Law, GR 71/2019, and MOCI Reg. 20/2016. However, please note that their applicability is limited **specifically** to the context of electronic system providers (such as providers of web portals, online platforms or applications, search engines, data hosts, etc.).

Current law dictates that electronic system providers that purport to process and/or obtain personal data are required to obtain the consent of the owner of the personal data as the fundamental basis for the lawful usage and processing of such data. The data processing activities envisaged must be sufficiently disclosed to the data owner and their consent must be given. Aside from obtaining consent, all electronic system providers must, among other actions, register with the MOCI, ensure the security and feasibility of their system infrastructure, and report any data breach to the MOCI, pursuant to the regulated procedures.

Please note that as of this writing, Indonesia has not promulgated a specific law on data protection which has universal scope of application, regardless of online or offline platform. The Indonesian Parliament (*Dewan Perwakilan Rakyat*) is discussing a draft bill on personal data protection. If enacted, the personal data protection draft bill would be the first comprehensive law in Indonesia to specifically deal with the protection of personal data. However, there is no certainty on when the bill will be enacted.

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

First and foremost, any processing of personal data, including the transfer of such data, whether within Indonesia or overseas, is prohibited unless the data owner has clearly provided their consent to the electronic system provider. The law requires any company/party that obtains and processes personal data to sufficiently disclose the data processing activities that will be done to such data. It also requires the data subject/owner to consent to these data processing activities in writing. Additionally, MOCI Reg. 20/2016 obliges the "consent form" to be in the Indonesian language. In practice, compliance with this rule is usually evident on online platforms, websites, or apps providing a bilingual privacy policy and consent form for users to consent by "clicking and accepting" such terms.

Aside from obtaining consent as the fundamental requirement, there is also a particular requirement related to the cross-border transfer of personal data by a domestic electronic system provider (domiciled in Indonesia), which is required to coordinate with the MOCI and ensure the "effectiveness" of its supervision "thereof". MOCI Reg. 20/2016 provides that the cross-border transfer of personal data by an ESP is subject to coordination with the MOCI or authorized officials/agencies. This coordination may be implemented by way of (a) coordinating with the MOCI or authorized officials, and (b) implementing the laws and regulations with respect to the cross-border transfer of data. The MOCI has not issued any further regulations clarifying this coordination requirement, be it with the MOCI or any other relevant institution. Consequently, there is as of this writing no affirmative action required on the part of business actors to satisfy this obligation. However, in practice, a number of business actors have managed to comply with the coordination requirement by sending a letter to the MOCI stating their plan to transfer personal data overseas. Following such transfer, these business actors then submitted a report to the MOCI stating that the transfer of personal data had been completed. There is no exact form for the letter required by the MOCI.

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

The EIT Law provides various fines depending on the type and severity of data breach. The maximum fine under the EIT Law is a criminal fine in the amount of IDR 12 billion (approximately USD 825,000) for breach of Article 35 of the EIT Law (i.e., intentionally and illegally manipulating, altering, omitting, or damaging electronic information and/or electronic documents so that it would be considered as if the data were authentic).

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

Indonesia's legal framework in the data protection realm is not as extensive as the GDPR. One example of this is that Indonesian laws do not recognize the concept of a data protection officer, in contrast to the GDPR.

Aside from that, as far as the current legal framework protects personal data, the protection afforded by the law is currently limited to electronic systems. That may change with the draft bill on general personal data protection still making its way through Parliament. Notwithstanding the above, we understand that the currently existing laws, e.g. GR 71/2019 and MOCI Reg. 20/2016, were drafted to mirror the GDPR.

19. Are there any regulatory guidelines or legal 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 GR 71/2019 and its implementing regulation on "public scope" electronic system providers, which are defined as state/governmental institutions that operate their own electronic systems, presumably for public and government-related functions.

Under this plain understanding, it is unlikely that the data-onshoring requirement would be imposed on cloud-based services, which are presumably not part of a "public scope" electronic system provider, but rather "private scope" ESPs, as defined in GR 71/2019. 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 public service electronic system providers, 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.

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

Under the EIT Law and GR 71/2019, 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 there are certain methods to show that the signatory has given consent for the relevant electronic information.

GR 71/2019 distinguishes between two types of electronic signature: certified and uncertified. While both are legally authentic and acceptable as long as they fulfill the above requirements, the main difference is that a certified electronic signature has stronger evidentiary value; some legal practitioners contend that it has the same evidentiary value as an authentic deed. This is crucial if the document is to be used in court proceedings where the parties need to prove the authenticity of the e-signature. Electronic signatures can be certified only by recognized providers. According to the MOCI website, there are currently seven Indonesian e-signature certification providers. They are the (i) Agency for the Assessment and Application of Technology (*Badan Pengkajian dan Penerapan Teknologi* or "**BPPT**"); (ii) State Code and Cyber Agency (*Badan Siber dan Sandi Negara* or "**BSSN**"); (iii) Perusahaan Umum Percetakan Uang Republik Indonesia (Perum Peruri); (iv) PrivyID; (v) Vida; (vi) Digisign; and (vii) Djelas. The first two institutions are government agencies, while the other five are state or private companies.

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

When outsourcing IT services, the employees, assets or third-party contracts remain with the outsourcing company unless otherwise regulated under the outsourcing contract or transferred in a separate transaction. Under the new manpower regulations following the issuance of the Job Creation Law, the possible automatic trasnfer of employment for failure to follow outsourcing regulations and laws no longer applies. An employer can outsource any work or manpower to any third party on commercial terms to which the parties agree.

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

As Indonesian law has yet to regulate artificial intelligence, reference must be made to 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 the entrepreneur. As such, in the event of an AI malfunction, the provider shall be liable for all damages suffered by the consumer. In terms of civil liability, the Indonesian Civil Code provides a general principle that the owner/master of a building or goods under its supervision shall be liable for any damages caused by such building or goods.

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

obligations as to the maintenance of cybersecurity

The Indonesian data protection laws, which consist of the EIT Law and GR 71/2019, require ESPs to ensure the security of the data they maintain and process. ESPs are to have security procedures, measures and infrastructure in place to prevent disruptions, failures, and damage within their electronic systems. However, the provisions under the data protection laws only contain a general obligation to maintain security. They do not stipulate an exhaustive list of mandatory security measures or go into further detail as to the minimum measures required for mandatory security procedures and infrastructure. More detailed sector-specific requirements are regulated by the relevant institution. For instance, cyber and data security obligations for cryptocurrency exchanges and online lending platforms may differ, pursuant to the respective regulations issued by Bappebti and the OJK.

a) 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 EIT Law and its

implementing regulations. The EIT Law 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 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 IDR 600 million (approximately USD 41,000) to IDR 800 million (approximately USD 55,000).

There is no tailored provision in the EIT Law for DDOS attacks. Instead, it falls under the general prohibition on "causing disruption to an electronic system and/or causing an electronic system not to function as it should." The possible legal consequence for such crime is a maximum imprisonment of 10 years and/or a maximum penalty of IDR 10 billion (approximately USD 690,000).

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

E-commerce ecosystems and their corresponding ecosystems (i.e., network and cellular data providers, data centers, software, cloud services/cloud computing, and infrastructure such as telecommunications towers) are becoming more and more important to the Indonesian economy, especially during the Covid-19 pandemic and the post-pandemic world. Such technology will most likely drive changes in other sectors as well, such as health services, insurance (through telemedicine, tele-health services, e-insurance platforms), education (through more e-learning platforms in the formal and informal education sectors), logistics, groceries, and so forth. We suspect the development of the legal framework will begin to accommodate the use of such developing technologies, where sectoral ministries will be required to jointly regulate certain matters. For instance, the MOCI along with the Ministry of Health and the Food and Medicine Supervisory Body may regulate different aspects of telemedicine services, the MOCI with the Ministry of Education and Culture for education, and so forth.

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

We believe that a major impediment to the development of technology and the economy is the continue lack of a specific law to govern the use and protection of personal data. Although the current GR 71/2019 and the MOCI's implementing regulations are said to mirror the best practices and provisions of the GDPR, their coverage is limited to electronic service providers (such as for websites, platforms, or applications). There is still no law that covers the protection of personal data outside of electronic systems. Historically, this has caused confusion among business players in the technology sector, particularly with regard to the level of compliance and security required to properly run their business in Indonesia. wherewith technology and data being applied in more fields of businesses the enactment of a law on personal data protection is crucial.

Another issue is the criminal provisions under the EIT Law, which stipulate criminal sanctions for personal defamation, online threats and religious blasphemy. In theory, these provisions are designed to enable the arrest and prosecution of cybercriminals. In reality, the EIT Law has been used to prosecute individuals for making defamatory or insulting statements online, which is subject to criminal prosecution. There is a perception among many people in Indonesia that the EIT Law has been used by regional authorities or the central government in Jakarta to silence citizens who have used online platforms to protest or criticize government policies. We understand from news reports that the government plans to revise the EIT Law to draw a clearer distinction between cybercrimes and non-criminal online actions, but we have yet to see any such revision.

Aside from the above, we note that the Government had taken some positive steps, especially in relation to foreign investment. For example, the MOCI used to impose a foreign shareholding limitation for the business line of online web portal for commercial purposes, under which a company could only be 100% foreign owned if it had minimum paid-up capital of IDR 100 billion. This limitation has been revoked by virtue of the new Indonesian Investment List, following the enactment of the Job Creation Law.

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

In more recent times, especially during the Covid-19 pandemic, we believe that Indonesia has encouraged

digital services, with a particular interests in e-commerce and financial technology. For instance, the MOCI and MOT have continued to develop the regulatory framework for e-commerce licensing and registration for electronic system providers, as they look to provide greater legal certainty to companies and protection for users, in particular their data.

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

There is at the moment no specific law or regulation that addresses the use of artificial intelligence. However, artificial intelligence is mentioned in Financial Services Authority (OJK) Regulation No. 13/POJK.02/2018 regarding Digital Financial Innovation in the Financial Services Sector, dated 16 August 2018, as one of the examples of digital financial innovation in the category of market support. Other examples of market support include machine learning, machine-readable news, big data, social sentiment, market information platform, and automated data collection and analysis. Outside the realm of financial technology, we understand that there is as of this writing no law or regulation that governs with universal scope the use of artificial intelligence and the consequences which may arise from such use.

Contributors

Fahrul S. Yusuf
Partner
fahrulyusuf@ssek.com

Albertus Jonathan Sukardi
Associate
albertussukardi@ssek.com