

Expert Analysis Chapters

1

De-risking Digital Business Dreams

James Gill, Victor Timon & Helen Hart, Lewis Silkin LLP

5

Modern Slavery: A 'Wicked Problem' that Requires a Human Rights-Based Approach

Anne O'Donoghue, Lihini Konara, Adelaide Falzon & Tiara Dalpadado, Immigration Solutions Lawyers

Q&A Chapters

15

Bahrain

Hassan Radhi & Associates: Ahmed Abbas & Sayed Jaffer Mohamed

20

Brazil

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados: Fabio Ferreira Kujawski, Lisa Worcman, Paulo Marcos Rodrigues Brancher & Thiago Luis Sombra

28

Canada

ROBIC LLP: Jean-François Normand

36

Cyprus

E & G Economides LLC: Xenia Kasapi & George Economides

43

France

Armengaud Guerlain: Catherine Mateu

54

Germany

SKW Schwarz: Dr. Christoph Krück, Franziska Ladiges, Alexander Möller & Heiko Wunderlich

62

India

G&W Legal: Disha Mohanty & Arjun Khurana

70

Indonesia

Bagus Enrico & Partners: Enrico Iskandar, Bratara Damanik & Jonathan Cheong

78

Ireland

Lewis Silkin LLP: Victor Timon

88

Italy

Portolano Cavallo: Irene Picciano, Fabiana Bisceglia, Donata Cordone & Livia Petrucci

97

Japan

Anderson Mōri & Tomotsune: Ken Kawai & Takashi Nakazaki

104

Malaysia

Shin Associates: Joel Prashant & Foo Jia Yi

116

Nigeria

Greychapel Legal: Eniola Elegushi & Maryann Ntamere

124

Romania

Mic, Ilie & Asociații / Pelinari & Pelinari / SLV Legal: Alexandru Stanescu, Andrei Pelinari, Stelian Mic & Tudor Velea

135

Saudi Arabia

Hammad & Al-Mehdar Law Firm: Suhaib Hammad

141

Switzerland

Walder Wyss Ltd: Jürg Schneider, Hugh Reeves & Maria Gentile

149

Taiwan

Lee and Li, Attorneys-at-Law: Robin Chang & Eddie Hsiung

156

United Kingdom

Charles Russell Speechlys LLP: Jason Saiban & Caroline Swain

164

USA

Cozen O'Connor: Victor J. Castellucci

Indonesia



Enrico Iskandar



Bratara Damanik



Jonathan Cheong

Bagus Enrico & Partners

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

The comprehensive umbrella regulation for the e-commerce ecosystem in Indonesia was enacted through Government Regulation No. 80 of 2019 (“**GR 80/2019**”) regarding Trade Through Electronic System / E-commerce (locally known as *Perdagangan Melalui Sistem Elektronik* – “**PMSE**”). The government enacted GR 80/2019 on 25 November 2019 and included a two-year transitional period for existing e-commerce businesses to ensure their operations were compliant with the regulation.

GR 80/2019 has defined any individual or entity – whether a legal entity or a non-legal entity, and which can be either local or foreign – conducting e-commerce activities as business actors (“**Business Actor(s)**”). The definition of Business Actors can also include foreign individuals or business entities incorporated and domiciled outside Indonesia which conduct e-commerce activities within the territory of Indonesia. Furthermore, the regulation has provided three classifications of Business Actors, namely:

- **Merchant:** A merchant is any Business Actor who conducts e-commerce activity (for commercial purposes and not on a temporary basis), either through its own electronic systems or through an electronic system of an e-commerce operator.
- **E-commerce Operator** (locally known as *Penyelenggara Perdagangan Melalui Sistem Elektronik* – “**PPMSE**”): An e-commerce operator is any Business Actor who provides a service and/or an electronic system to facilitate an e-commerce transaction. This may also include any merchant who also provides its own electronic system when conducting e-commerce activity. Other types of business model which can be categorised as an e-commerce operator include online marketplace platforms, online classified ads, price comparison platforms and daily deals.
- **Intermediary Service Operator (“ISP”)**: An intermediary service operator is any Business Actor that provides

intermediary or indirect services to support e-commerce activities, including search engine providers, hosting providers and caching providers.

While there is not yet a legal obligation specifically directed to B2B e-commerce under the prevailing laws and regulations, the government has issued Minister of Trade Regulation No. 50 of 2020 regarding Provisions on Business Licensing, Advertising, Guidance and Supervision of Businesses in Trade through Electronic Systems (“**MoT 50/2020**”) as an implementing regulation of GR 80/2019. Under MoT 50/2020 and GR 80/2019, there are obligations and requirements that must be fulfilled by certain parties, either individual or entities, involved in e-commerce (including B2B and B2C e-commerce), as follows:

- a) **General obligations**
 - compliance with applicable regulation on taxation, data protection, import/export activities, consumer protection and advertising ethics;
 - compliance with general business requirements (for example, technical licences, standardisation of goods/services, among other vital factors);
 - assistance with government programmes, if requested (e.g., prioritisation of the trading of domestically produced goods/services);
 - provision of terms of use or the licence agreement to their users; and
 - provide means of technological control and/or means of receiving public complaints regarding the existence of illegal electronic information in their electronic system in accordance with provisions of applicable laws and regulations.
- b) **Licensing and Registration Requirement**
Under MoT 50/2020, particularly for domestic PPMSEs, non-exempt ISP and domestic merchants that have their own electronic communication facilities used for trade transactions must obtain a specific licence prior to conducting operation in Indonesia, i.e. Trading Business License Through an Electronic System (locally known as *Surat Izin Usaha Perdagangan Melalui Sistem Elektronik* – “**SIUPMSE**”). To secure a SIUPMSE, the Business Actor shall apply to the Minister through the Online Single Submission (“**OSS**”) system.

However, such SIUPMSE shall only be effective upon satisfaction to the following commitments/requirements:

- obtainment of Electronic System Registration (locally known as *Pendaftaran Sistem Elektronik*) Certificate issued by the Ministry of Communications and Informatics (“MCI”) within 14 working days after the issuance of SIUPMSE.
- Electronic System Registration is a straight-forward process which is conducted within MCI’s online system. The registration requires several corporate documents which include, among others: (a) registration form; (b) corporate documents; (c) applicant’s profile; and (d) brief information on the technicality of the Platform. Following the submission of those documents, MCI will generally be able to issue the certificate within seven business days;
- provision of website address and/or application name;
- establish accessible consumer service’s contact details, i.e. contact and/or email address; and
- establish a consumer service which contains contact details of Directorate General of Consumer Protection and Trade Compliance.

In addition, a PPMSE can use an electronic certificate in relation to an e-commerce transaction. There is no mandatory requirement to use an electronic certificate issued by the authorised Indonesian electronic certification organisers; however, the government will not view an e-commerce transaction which uses an electronic certificate issued by foreign electronic certification organisers as authentic evidence in Indonesia.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

Please revert to our answer to question 1.1 as it is also applicable to B2C e-commerce.

Additionally, in doing B2C e-commerce, GR 80/2019 stipulates some standards related to offers, acceptances and confirmations. Each of these provisions possess specific criterion, as follows:

- a) An offering shall be valid and have binding legal force if there is a clear and specific statement of intention in the offering, as well as terms and conditions, by way of truthful, fair and balanced offerings, as well as certain time restrictions.
- b) Acceptances are deemed to be accepted is if the accepting party already shows that it has accepted the terms and conditions delivered in the offerings.
- c) Confirmations can be electronic or non-electronic given by Business Actors to consumers as a response to the consumers’ acceptance. The contents of a confirmation must be the same as the offering information.

Particularly in the case where the PPMSE is a foreign individual or business entity incorporated and domiciled outside of the territory of Indonesia, but actively conducting offerings to consumers residing within Indonesia, GR 80/2019 has put certain thresholds which may classify the abovementioned foreign Business Actor as physically present and operational as a permanent business establishment in Indonesia, such as: (i) transaction volume; (ii) transaction value; (iii) volume of packages to be shipped; and/or (iv) volume of traffic or people who access the foreign Business Actor. Once the foreign PPMSE

has satisfied the criteria above, they will be required to appoint an Indonesia representative that will act on their behalf in the form of Representative Office of Foreign Trade Companies (locally known as *Kantor Perwakilan Perusahaan Perdagangan Asing* – “**KP3A**”) within the sector of Trade through Electronic.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Through 2020, there was no new and/or updated data protection regulation. The latest regulations issued in 2019, which partially cover data issues, include:

- i) Government Regulation No. 71 of 2019 regarding Implementation of the Electronic System and Transaction (“**GR 71/2019**”), an update and replacement to the obsolete Government Regulation No. 82 of 2012 regarding the same;
- ii) Government Regulation No. 80 of 2019 regarding trade through electronic systems (“**GR 80/2019**”);
- iii) Ministry of Communications and Informatics (“MCI”) Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic System (“**MCI Regulation 20/2016**”); and
- iv) Law No. 11 of 2008 regarding Electronic Information and Transaction as lastly amended by Law No. 19 of 2016 (“**EIT Law**”).

Even though the latest regulations have been enacted, i.e., GR 71/2019 and GR 80/2019, it does not cause radical changes to the currently prevailing data protection environment in Indonesia; however, both show the Indonesian government’s emphasis on the importance of data protection regulations within Indonesia’s regulatory framework.

For your reference, the Indonesian government has already drafted and submitted a draft bill on data protection (“**PDP Bill**”), in which approval is being deliberated. Enactment of the PDP Bill would establish more detailed rulings on data protection. Enactment of the PDP Bill may effectively introduce new provisions similar to the EU General Data Protection Regulation.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

In general, the main challenges happened due to the absence of comprehensive rulings in data privacy and data protection in Indonesia, as we will describe below.

a) **Financial Technology (Fintech)**

Fintech that has been developed in Indonesia include, among others: (i) online payment; (ii) peer-to-peer lending; (iii) insurance-tech; (iv) aggregator; and (v) crowdfunding. Such type of Fintech is closely supervised by our central bank (Bank Indonesia – “**BI**”) and financial authorities (Financial Services Authorities, locally known as *Otoritas Jasa Keuangan* – “**OJK**”) through a regulatory sandbox and determined based on the nature of its transaction. We understand that the lack of data privacy and data protection regulation has hindered certain Fintech companies in providing services to their consumers. However, the regulator has set certain requirements to reduce the risks that might occur for Fintech companies who will operate in Indonesia, including to maintain the confidentiality of consumer data and/or transaction data. For instance, in

the absence of such rulings, there is a case where Fintech companies particularly those operating in peer-to-peer lending are restricted by OJK to only have access to certain consumers' personal data when providing services through a smartphone application i.e., camera, microphone, location.

b) Digital Health

Currently, the provisions related to digital health privacy are only on the management of a patient's 'medical records', which is regulated under Ministry of Health Regulation No. 269 of 2008 regarding Health Records. Medical record incorporates several pieces of information, among others: patient's identity, diagnosis, anamnesis/medical history, examinations history, and medication history (hereinafter referred as "**Patient Data**"). The concept of data privacy in the healthcare sector is slightly different to data privacy in general due to fact that the medical record document is owned by the healthcare provider; however, please note that the content of the medical record is still owned by patients. Thus, any disclosure of Patient Data must be authorised by the patient.

c) Other Sectors (i.e., Retail and AI)

Regarding retail and AI, being relatively new concepts, these are yet to be specifically governed by significant regulations that oversee and tackle the vast privacy issues.

As to the extent of utilising collected data, it is extremely important to first provide an explanation on the purpose of collection and obtain consent from the data owner.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?

While retail, AI and digital health have not yet been given significant attention in Indonesia's regulatory framework, BI and OJK provide a regulatory sandbox for Fintech companies to test their products, services, technologies, and business models under their supervision. In order to accommodate the innovative products provided by Fintech companies, and in the absence of specific regulation, both BI and OJK have their own regulatory sandbox in which Fintech companies are able to operate under special exemptions for a limited period of time. Under the practice, Fintech companies who are connected to payment systems are under BI's jurisdiction, while others (outside of payment systems), such as insurance-tech, peer-to-peer lending, robot advisory, or credit scoring services, will be under OJK's jurisdiction.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

The prevailing legal framework for cybersecurity in Indonesia is dispersed within various regulations. Nonetheless, the main reference for cybersecurity in Indonesia is Law No. 11 of 2008 regarding Information and Electronic Transactions as lastly amended by Law No. 19 of 2016 ("**EIT Law**"). However, EIT Law regulates more so on the prohibition of cyber incidents (including hacking, denial-of-service, phishing, identity theft), rather than outlining the specific forms of cybersecurity that can be applied in Indonesia. Depending on the context, other regulations may have specific cybersecurity framework applicable to e-commerce businesses.

In relation to personal data, in 2016, the Ministry of Communication and Informatics ("**MCI**") enacted specific regulation through MCI Regulation 20/2016. MCI Regulation 20/2016 requires all electronic system operators in Indonesia to store any personal data in its possession in an encrypted form, although there is no further stipulation on the encryption mechanism to be implemented. This is also directed to the e-commerce sector, which, to an extent, is stipulated in GR 80/2019 where an e-commerce operator can use encryption or cryptographic products in e-commerce activity.

Meanwhile, under GR 71/2019, any parties which provide, manage, and/or operate electronic systems for their own purposes and/or for other parties' purposes would be categorised as an Electronic System Operators ("**ESOs**"). As such, e-commerce operators are also considered ESOs and are obliged to implement measures to protect their electronic system operational activity, wherein they must:

- provide an audit trail for all activities of the electronic system for the purpose of supervision, law enforcement, dispute resolution, verification, testing and other examinations;
- conduct security checks for the components of the electronic system;
- own and operate procedures and facilities for the security of the electronic system in preventing disturbance, failure and loss;
- maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information and/or electronic documents; and
- provide features in accordance with the characteristics of the utilised electronic system at least in the form of facilities to: (i) make corrections; (ii) cancel a command; (iii) provide a confirmation or reconfirmation; (iv) choose to continue or to stop the next activity; (v) view the submitted information in the form of an electronic contract offer or advertisement; (vi) check the success or failure of an electronic transaction; and (vii) read the agreement before conducting an electronic transaction.

A notable mention that may affect the future of cybersecurity is that the government previously submitted a draft bill on cybersecurity in 2019 which failed to fulfil the requirements to be enacted. However, to date, there is no clear timeline on the enactment of such draft bill in the future.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

a) Financial Services Sector

The use of information and technology in the banking sector is regulated under Financial Services Authority No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks as lastly amended by OJK Regulation No. 13/2020 ("**OJK Regulation 38/2016**"). The following are examples of compliance requirements under OJK Regulation 38/2016 that are related to cybersecurity matters:

- forming an Information Technology Steering Committee;
- at least once a year, performing a trial of a Disaster Recovery Plan involving all critical applications and infrastructures in conformity with the business impact analysis result;

- background check of criminal records during the recruitment of IT staff, including staff of the IT service provider, and network administrator or system administrator positions;
- to have an IT operational security procedure;
- consider the formation of an Incident Response Team in Information Security, in accordance with the bank's business complexity;
- within seven days after the event has come into realisation, reporting any critical events, abuse, and/or criminal offences in the implementation of information technology which may and/or have caused significant financial losses and/or disrupted the bank's operational continuity, in the form as stipulated by OJK; and
- a Data Centre/Disaster Recovery Centre may be located outside the territory of Indonesia, provided that an approval from OJK has been obtained; such approval will be granted subject to satisfaction of certain requirements.

Any non-compliance with such provisions may be subject to penalties in the form of administrative sanctions and fines.

b) Telecommunications Sector

The procedures for telecommunication services are regulated in MCI Regulation No. 13 of 2019 regarding Implementation of Telecommunication Services. The regulation provides that the Telecommunications Service Provider is required to make the following efforts as a form of implementation of cybersecurity:

- use telecommunication tools and/or devices that have met specified and certified technical requirements;
- the Telecommunications Service Provider must keep customer data at least in the form the customer's name and customer identification number; and
- for the purposes of the criminal justice process, the Telecommunications Service Provider is obliged to keep recorded data directly related to the court process referred to until the court decision is legally binding.

c) National Strategic Sector

According to Presidential Regulation No. 133 of 2017 regarding Amendment to Presidential Regulation No. 53 of 2017 regarding State Cyber and Code Agency ("BSSN"), BSSN is a government institution that carries out cybersecurity as effectively and efficiently as possible by utilising, developing and consolidating all elements related to cybersecurity. BSSN coordinates with all ministries within the cabinet including the national critical industries, such as ICT, energy, transportation, health, national defence and security, in order to enforce their scope of cyber protection. Furthermore, to secure an operation in every electronic system, BSSN has enacted BSSN Regulation No. 8 of 2020 regarding security system in the operation of electronic system ("BSSN Regulation 8/2020"). It stipulates that every ESO operated in Indonesia is required to comply with the implementation of information security management based on the principal risk (locally known as *Sistem Manajemen Pengamanan Informasi* – "SMPI"). SMPI standards will be adjusted to the level/category of relevant electronic system i.e.: (i) strategic; (ii) high; and (iii) low. For your reference, the higher the level/category of the electronic system, the more complex the standards that need to be applied, such as: (a) SNI ISO/IEC 27001; (b) other security standards related to cybersecurity established by BSSN; and (c) other security standards related to cybersecurity established by the Ministry or Institution.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

The COVID-19 pandemic has undoubtedly caused a huge shift towards consumers' attitudes towards e-commerce. According to a Bank Indonesia survey, the value of e-commerce transactions reached a record-high of USD18.2 billion, a modest 29.6% increase from USD14 billion in 2019 despite the negative sentiment brought by the pandemic. Such increase is also coupled with a boost in the usage of e-wallet/digital payment methods.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

According to a 2020 Bank Indonesia report, the most favoured payment method for e-commerce transaction is e-wallet/digital payment with 41.71% usage, while the more conservative bank transfers and cash-on-delivery payment method accounts for only 20.23% and 19.01%, respectively. Consistent with payment in the e-commerce sector, the use of cashless payment methods is also significantly increasing today with many consumers avoiding direct contact during the ongoing COVID-19 pandemic, which can be seen from some surveys highlighting significant increases of new users in some e-wallet and digital payment service providers in Indonesia throughout 2020.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

We believe that in some countries which already have a more advanced and detailed IT-related regulatory framework (e.g., on data protection and cybersecurity), home-state retailer websites/e-commerce platforms may perform better. For example, in Indonesia, if a new type of financial-related business model that is meant to support an e-commerce business is not covered in any regulation, it will need to obtain a regulatory sandbox approval from the relevant authority. In order to obtain the approval, it will have to go through an initial inspection and analysis of the platform, which may take significant time.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Most Indonesian e-commerce platforms are still displayed in the Indonesian language only (*Bahasa*), as currently most Indonesian e-commerce business still target domestic consumers and it can also be seen that most Indonesian e-commerce firms do not provide an option for international shipping. This is also due to the mandatory requirement of presenting information of the operation of electronic systems in an understandable manner, including using Bahasa within electronic contracts that are addressed to Indonesia's consumers.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

As in most jurisdictions, having web-interface concepts presented in the local language is always the first stage in order to appeal to the specific market. Other design concepts that may impact consumer interactivity truly depend on the specific market and product that is being sold and marketed.

4.6 Has the Covid-19 pandemic had any lasting impact on these cultural norms?

Yes, especially in the payment method and e-commerce sector. Previously, cash on delivery was popular and often used as the preferred payment method. The same goes for offline shopping, where many still preferred to shop directly at retail stores. However, the COVID-19 pandemic has significantly shifted the trends, and we are seeing that cashless payment methods and online shopping are becoming more and more preferable today.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

In order to obtain protection for a brand, a brand owner should first register its product's trademark to the Indonesian Trademark Office. Once the trademark office validates the registration, the registered brand/trademark will be protected for a period of 10 years and can be renewed. Further, as Indonesia is also a contracting party to the Protocol relating to the Madrid Agreement on the International Registration of Trademarks, a foreign brand owner can register an international brand in Indonesia through the international bureau, provided that it has commercial activity in Indonesia.

The Ministry of Law and Human Rights ("MoLHR") and MCI jointly issue Decree No. 14 of 2015 and No. 26 of 2015, respectively, regarding the Implementation of Closing Down Content and/or User Right to Access on Copyright Infringement and/or Related Rights in Electronic System. The joint decree stipulates, among others, the procedure on filing a report on copyright infringement in electronic systems, the verification procedure of filed reports, as well as the procedure for closing down the content and/or access rights related to copyright infringement. Furthermore, GR 80/2019 also provides that PPMSE can be held responsible for any illegal contents within their platforms, although such responsibility does not apply if the PPMSE swiftly removes such illegal contents at the first instances after it became aware of such illegal content within their platforms.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Trademark law only gives the right to a registered trademark owner or an unregistered famous trademark owner to file a lawsuit regarding its trademark infringement. Additionally, a trademark owner may also file a lawsuit to a facilitator or re-seller of counterfeit goods or unlicensed services.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

Indonesia data protection regulation has not yet provided a detailed outline of the division of responsibilities between a data controller and a data processor. Accordingly, as data processed or stored by third-party data centres or cloud providers are collected by a service provider (as data controller), any mishandling or privacy breach conducted by the third-party data centres or cloud providers may fall under the service provider's responsibility.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Generally, electronic service providers may locate their data centres outside Indonesia and send personal data to an area outside Indonesia, provided that the area has been declared as having the same protection level and standard as Indonesia by the relevant authority. However, stricter additional requirements of data localisation may apply to electronic service providers in public sectors and other specific sectors, such as the financial sector.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

Whilst currently there is no one specific type of technology being adopted, there are numerous efforts carried out by the government specifically focused on logistics, consumer protection and other e-commerce matters in order to accommodate the rapid growth of the digital market. The issuance of GR 80/2019 is one of the key regulations mandated under Presidential Regulation No.74 of 2017 on the National E-Commerce Road Map 2017–2019 ("PR 74"). Enactment of this specific regulation provides great clarity through improvements in the government's governance related to the increasingly rapid development in all e-commerce practices within Indonesia.

Nevertheless, under the Indonesia blueprint on National Logistic System, there will be more utilisation of technology and further development of MSME logistics data transfer to ensure further digitalisation of international trade in Indonesia. The government wants to develop a National e-Logistics which would provide services such as the transfer of data, logistics documentation and any reliable information in order to facilitate G2G, B2G and B2B transactions, either domestic or international, by also connecting with ASEAN and global logistic networks.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

Indonesia, being one of the fastest growing digital market economies in the South East Asian region, continuously strives to overcome barriers and accommodate rapid growth of the digital economy. Notable aspects that must be accounted for include the encompassment and facilitation of the different desires of

customers and demographics, improvements on data analytics and cybersecurity. These are key factors that continually enable Indonesia to further advance in such a large e-commerce sector. The government has already begun to anticipate such growth by the revolutionary enactment of GR 80/2019, which comprehensively stipulates the guidelines governing extensive matters relating to e-commerce within Indonesia, including compliance checklists for e-commerce businesses. GR 80/2019 has been key in establishing the clarification of the different recognised e-commerce parties, requirements for e-commerce business practitioners, and the importance of consumer protection obligations, including enforcement of personal data protection requirements.

Note that in the near future there may be further regulations governing trade practices such as taxation and logistics.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

The Ministry of Finance (“**MoF**”) in Indonesia has provided several tax incentives (such as tax allowance and tax holiday) on income tax that are applicable to relevant digital businesses. The award of such tax incentives is subject to the MoF’s approval following the fulfilment of certain requirements, among others: (i) the nature of business is part of a pioneering industry which is entitled to such tax incentive; and (ii) the business’ investment value in Indonesia will determine the amount and period of tax holiday.

Unfortunately, there has not yet been a tax incentive in relation to research and development conducted by entities; however, we understand that there is an ongoing discussion between government entities on regulating such tax incentive.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

Previously, the government did not specify the taxation mechanisms specific to over-the-top (“**OTT**”) service providers that operate remotely outside of Indonesia.

For instance, under the current prevailing law and regulations, foreign digital businesses (including Business Actors) will be required to collect and deliver value added tax (“**VAT**”) to the tax authority by appointing a representative in Indonesia. Additionally, a foreign digital business which is categorised as having a significant economic presence in Indonesia is to be treated as a permanent establishment, which will be subject to income tax. The criteria used to determine significant economic presence are (i) gross distribution of business group consolidation, (ii) sales value within the Indonesia territory, and/or (iii) active users of digital media in Indonesia.

Furthermore, due to the COVID-19 pandemic, the Indonesian Government has decided to accelerate the tax collection on overseas digital businesses by enacting Government Regulation No. 1 of 2020 relating to Financial State Policy and Stability of Financial System during the Coronavirus Disease (“**GR No. 1/2020**”). GR No. 1/2020 has incorporated the above criteria of foreign digital businesses having significant economic presence in Indonesia who shall comply with prevailing income tax or an electronic transaction tax. Furthermore, any utilisation of non-material taxable goods and/or taxable services from outside custom areas to within custom areas through an e-commerce system will

be subject to prevailing VAT regulations. Those failing to comply with the above shall be subject to a warning, administrative sanction and a potential access termination upon businesses’ electronic systems by MCI.

Clarification of procedures as above-mentioned have been provided through the enactment of the implementing regulation of PER-12/PJ/2020 on Certain Criteria relating to the Appointment of Collectors, Collection, and Deposit, and Reporting of Value Added Tax in the Utilization of Intangible Taxable Goods and/or Taxable Services from Outside of Customs Area in the Customs Area Through Trade via Electronic Systems (“**PER-12/PJ/2020**”). This has solidified that generally digital businesses and any other foreign services are subjected to electronic tax due to sales of digital products by overseas sellers to consumers within the customs area of Indonesia. Foreign OTT services will be charged with VAT (or locally known as *Pajak Pertambahan Nilai*) of 10% from the transaction value as per the taxation policies of the Directorate General of Taxes (“**DGT**”). This VAT rate is applied at the point-of-sale against the taxable amount which is the amount payable by the customer before any taxes.

Digital products/services included, but not limited to:

- movies, music, and other audio-visual contents;
- computer software, mobile apps, games;
- electronic books, magazines, and comics;
- web hosting;
- videoconferencing services; and
- other services delivered through computer networks.

Although GR No. 1/2020 was originally issued to ensure economic stability during the COVID-19 pandemic, it provides us with a better view on how the government will regulate the taxation for foreign digital businesses in the future.

The regulations have provided clarity related to the amount of the tax fee, collection procedure, representative appointment procedure, and thresholds for determining significant economic presence for digital business and OTT services. Despite the clarifications, it will undoubtedly take time for the government’s significant enforcement of these taxation policies. Nevertheless, it is fair to state that there are no longer any misconceptions or disputes as to whether specific digital businesses and/or OTT services are to be taxed.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

There are two types of employment status based on Law No. 13 of 2003 regarding Manpower (“**Manpower Law**”), namely: Specified Time Work Agreement (“**PKWT**”); and Permanent Work Agreement (“**PKWTT**”). The difference between the two agreements lies in the agreed working period. A PKWT is given for certain types of work which are temporary and relatively short. The contract period is for a maximum of five years. The termination of the PKWT and PKWTT made by the company causes the company to pay certain severance payments.

Manpower Law also stipulates that companies that hire employees for supporting activities and not the main activity of the company (e.g. chauffeurs, housemaids, etc.) can contract their employees either on a PKWT or PKWTT through outsourcing. An advantage of outsourcing is the recruitment process where

companies are able to reduce their budget and the time taken to hire as it is the paid responsibility of the service provider.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There are no specific laws and regulations governing work performed outside of the office. Manpower Law gives employees and employers the freedom to determine their own policies in carrying out jointly agreed business activities in work contracts, company regulations and collective labour agreements.

9.3 What long-term effects or changes are likely to result from the Covid-19 pandemic?

Due to the COVID-19 pandemic, the Indonesian government has enacted several new manpower regulations in continuation with the Omnibus Law for the purpose of attracting more investments into Indonesia. As the previous manpower regulations were quite rigid and the regulations were deemed more beneficial to employees compared to businesses, the newly enacted manpower regulations have set further details in case of an employee's termination, including the calculation of the termination package for each event of termination. This has provided further confidence to employers since the calculation of termination package is seen more reasonable compared to that in the previous regulation.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

The amount of dispersed regulations relevant to digital business may affect the development of an e-commerce ecosystem. Since the relatively recent enactment of GR 80/2019, digital businesses now have a clearer vision on various legal aspects such as requirements, registration, payment methods, formation of electronic contracts, consumer protection and mechanisms of resolving disputes within the e-commerce realm that must be abided by. Put aside the implementation of regulation GR 80/2019, the government has also prepared a draft bill on data protection which will impose further obligations on digital businesses. It is important for the government to find a balance in protecting the interest of the e-commerce ecosystem by providing regulatory effectiveness in the era of digitalisation.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Indonesia being the fourth most populous nation in the world, and having the largest population in Southeast Asia, holds endless advantages for any digital business looking to expand their operations. As one of the biggest e-commerce economies in Southeast Asia, Indonesia's e-commerce industry is expected to reach USD40 billion by 2022 and is estimated to see an additional estimated 42.1 million e-commerce shoppers by 2021. An estimation by global tech giants Google and Singapore's Temasek places Indonesia's e-commerce economy at USD53 billion in 2025.

We believe digital businesses are capable of utilising and investing in some of the advantages offered in Indonesia,

including: (i) secure and scalable payment opportunities; (ii) large, strong talent pool; and (iii) an increasing digital-commerce ecosystem. These factors will provide great advantages for digital businesses operating in Indonesia.

10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?

The Indonesian regulator is currently focusing on establishing the detailed regulatory framework on data protection as more businesses in Indonesia collect and process personal data. The discussions on the bill of personal data protection has been ongoing for the last couple of years; however, the enactment of such bill has not materialised until to date.

Furthermore, the regulator is also preparing a specific licensing framework for foreign digital businesses, where such businesses will still need to conduct certain registration such as Electronic System Registration and specific registration for foreign offshore entity. Therefore, OTT service providers may generally provide their services directly from offshore but with certain registration and compliance requirements in Indonesia.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

Generally, GR 80/2019 covers provisions on online payments related to e-commerce activity in Indonesia. E-commerce firms may provide an online payment option as one of its payment methods, by engaging in a partnership agreement with an online payment provider which has obtained approval from an authorised financial institution such as Bank Indonesia (as the Indonesian central bank).

Therefore, for the online payment sector, there are several regulations which may apply, among others: (i) Bank Indonesia Regulation No. 22 of 2020 on Payment System; (ii) Bank Indonesia Regulation No. 18 of 2016 on Operation of Payment Transaction Process; (iii) Bank Indonesia Regulation No. 20 of 2018 on Electronic Money; and (iv) Bank Indonesia Regulation No. 19 of 2017 on Operation of Financial Technology.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

The issue was mainly focussed on the various infrastructure of e-money payments where e-money providers develop their own products and subsequently, in certain cases, they were able to have exclusive partnerships with several merchants in order to prevent the use of other e-money. However, this has been resolved by the utilisation of National Payment Gateway in Indonesia where the government has established interconnected switching and guarantee the interoperability of each payment channels.

Another thing which should be noted is that whilst the government does not prohibit overseas delivery and purchases, all payments conducted by any parties that concern Indonesia are subject to the obligatory use of the Indonesian Rupiah only. New types of payment methods are yet to be recognised by any prevailing regulation. An example is the use of cryptocurrencies, which is recognised as a form of payment in a small number of jurisdictions. However, cryptocurrencies are not recognised by law as a form of payment in Indonesia.



Enrico Iskandar is a founding partner of Bagus Enrico & Partners, a firm which advises companies in corporate and commercial transactions, with an emphasis on mergers and acquisitions, corporate restructurings, property, hotels and real estate, technology, media and telecommunications.

In his technology, media and telecommunications practices, Enrico has worked on a broad range of transactional, advisory and contentious matters, and regularly advises on regulatory issues on telecommunications (including market entry advice), networks and satellite operations, data protection/privacy, cloud data, payments, outsourcing, IT contracts, e-commerce, IoT and supply chain transactions. Enrico's considerable experience in relation to technology, media and telecommunications has enabled him to steer investors through inherent practical and regulatory hurdles.

Enrico's team has been recognised by the Asia Pacific Legal 500 over the last five years (2017–2021 editions) as Indonesia's 1st Tier law firm in IT & Telecoms practice. He has also been recognised by The International Who's Who Legal for the last seven years (from 2013 to 2019), as a leading individual in Data, Information Technology and Telecoms & Media practices.

Bagus Enrico & Partners
 DBS Bank Tower 17th Floor, Suite 1701
 Jl. Prof. Dr. Satrio Kav. 3-5
 Jakarta 12940
 Indonesia

Tel: +62 21 2988 5959
 Email: enrico@bepartners.co.id
 URL: www.bepartners.co.id



Bratara Damanik is a senior associate of Bagus Enrico & Partners who has been primarily involved in various work in the technology, media and telecommunication areas. In addition, he also regularly advises clients within a wide spectrum of corporate and commercial matters on various sectors including M&A, construction, employment, as well as advising numerous corporate clients.

Bratara has been involved in a broad range of advisory work on regulatory issues regarding data protection, telecommunications and networks operation, IT contracts, cloud services, and in the e-commerce and fintech industries. He has also shown particular interest in the tech industry by studying and writing his master's thesis on blockchain at Queen Mary University, London.

Particularly for the technology sector, Bratara's recent representations include advising a major US-based tech company in the preparation of a streaming service activity in Indonesia and assisting venture capitals on their financing transactions into Indonesian-based tech companies.

Bagus Enrico & Partners
 DBS Bank Tower 17th Floor, Suite 1701
 Jl. Prof. Dr. Satrio Kav. 3-5
 Jakarta 12940
 Indonesia

Tel: +62 21 2988 5959
 Email: bratara@bepartners.co.id
 URL: www.bepartners.co.id



Jonathan Cheong is a consultant at Bagus Enrico & Partners. He is heavily involved in numerous works pertaining to assisting both international and local clients on several non-contentious matters in relation to Technology, Media, Telecommunications (TMT) and digital businesses.

He undertakes works comprising advisory and legal compliance related to regulatory matters including data protection, cybersecurity, and IT contracts. Some of Jonathan's work includes advisory for an international tech company in their market entry strategy whilst ensuring compliance to the existing legal frameworks. His most recent matter encompassed representational and advisory work for the potential entry of a US-based cryptocurrency. He is also the coordinator for the firm's publications and articles which are published on regulatory research platforms and legal guides.

Bagus Enrico & Partners
 DBS Bank Tower 17th Floor, Suite 1701
 Jl. Prof. Dr. Satrio Kav. 3-5
 Jakarta 12940
 Indonesia

Tel: +62 21 2988 5959
 Email: jonathan@bepartners.co.id
 URL: www.bepartners.co.id

Bagus Enrico & Partners ("BE Partners") is one of Indonesia's leading corporate and commercial law firms. Founded by professionals who are recognised for their experience in handling various notable transactions in Indonesia, BE Partners continues its growth with an equal commitment to our reputation as a "boutique practice focuses on client service", and provides its domestic and international clients with high-quality advice which is commercially focused and personally delivered.

BE Partners has received recognition from the main legal market reviewers. Some of the most international and respected reviewers have placed BE Partners' team as Indonesia's leading professionals in various practices. BE Partners' reputation in diverse aspects of Indonesian law, especially in relation to corporate/commercial law, banking, finance and insurance,

mergers and acquisitions, IT, media and telecommunications, energy and resources, property, hotels and real estate, as well as infrastructure, is outstanding.

www.bepartners.co.id



ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business

Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law

Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms