

# e-Commerce 2020

Contributing editor  
Robert Bond



**Publisher**

Tom Barnes

tom.barnes@lbresearch.com

**Subscriptions**

Claire Bagnall

claire.bagnall@lbresearch.com

**Senior business development managers**

Adam Sargent

adam.sargent@gettingthedealthrough.com

Dan White

dan.white@gettingthedealthrough.com

**Published by**

Law Business Research Ltd

87 Lancaster Road

London, W11 1QQ, UK

Tel: +44 20 3780 4147

Fax: +44 20 7229 6910

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between June and July 2019. Be advised that this is a developing area.

© Law Business Research Ltd 2019

No photocopying without a CLA licence.

First published 2000

Sixteenth edition

ISBN 978-1-83862-138-4

Printed and distributed by

Encompass Print Solutions

Tel: 0844 2480 112



---

# e-Commerce

## 2020

**Contributing editor****Robert Bond****Bristows LLP**

---

Getting the Deal Through is delighted to publish the sixteenth edition of e-Commerce, which is available in print, as an e-book, and online at [www.gettingthedealthrough.com](http://www.gettingthedealthrough.com).

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Getting the Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes a new chapter on Croatia.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at [www.gettingthedealthrough.com](http://www.gettingthedealthrough.com).

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editor, Robert Bond of Bristows LLP for his continued assistance with this volume.



London

July 2019

---

Reproduced with permission from Law Business Research Ltd

This article was first published in August 2019

For further information please contact [editorial@gettingthedealthrough.com](mailto:editorial@gettingthedealthrough.com)

# Contents

<b>Brazil</b>	<b>3</b>	<b>Malta</b>	<b>69</b>
Raphael de Cunto, Pedro Paulo Barradas Barata, Beatriz Landi Laterza Figueiredo, Luís Antônio Ferraz Mendes and Ana Carolina Fernandes Carpinetti Pinheiro Neto Advogados		Olga Finkel, Robert Zammit, Erika Micallef and Nicole Sciberras Debono WH Partners	
<b>Chile</b>	<b>13</b>	<b>Norway</b>	<b>81</b>
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya Magliona Abogados		Jeppé Songe-Møller, Kaare M Risung, Trond Larsen, Øivind K Foss and Marie Berggren Hagberg Advokatfirmaet Schjødt AS	
<b>China</b>	<b>22</b>	<b>Poland</b>	<b>91</b>
Jihong Chen Zhong Lun Law Firm		Robert Matecki and Jan Wiegner Matecki Pluta Dorywalski i Wspólnicy Spk	
<b>Croatia</b>	<b>34</b>	<b>Russia</b>	<b>100</b>
Irina Jelčić, Iva Burić and Paula Jagar Hanžeković & Partners Ltd		Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Kseniya Lopatkina, Vasilisa Strizh, Kamil Sitdikov and Brian L Zimble Morgan, Lewis & Bockius LLP	
<b>India</b>	<b>42</b>	<b>Switzerland</b>	<b>110</b>
Hardeep Sachdeva and Priyamvada Shenoy AZB & Partners		Lukas Morscher and Nadja Flühter Lenz & Staehelin	
<b>Indonesia</b>	<b>53</b>	<b>United Kingdom</b>	<b>122</b>
Fahrul S Yusuf and Mohammad K Bratawijaya SSEK Legal Consultants		Robert Bond Bristows LLP	
<b>Japan</b>	<b>61</b>		
Kozo Yabe and Takeshi Kanda Yuasa and Hara			

# Indonesia

Fahrul S Yusuf and Mohammad K Bratawijaya

SSEK Legal Consultants

## LEGAL AND REGULATORY FRAMEWORK

### Government approach

1 | How can the government's attitude and approach to internet issues best be described?

The Indonesian government initially adopted a conservative and relatively traditional approach to regulating internet-based activities. Prior to 2008, there was no legislation or guidelines in Indonesia that regulated the internet and how electronic information was offered and consumed, for both commercial and non-commercial purposes. In the five to seven years before 2008, Indonesia experienced the rapid development of information technology and the number of internet users in the country soared as the internet became the most popular medium to access electronic information. In response to this growth, the Indonesian government issued an underlying regulation to address potential issues resulting from activities conducted on the internet. On 21 April 2008, through the House of Representatives, the Indonesian government issued Law No. 11 of 2008 on Electronic Information and Transactions (the ITE Law).

The idea behind the ITE Law was to set out basic rules and provide a generic understanding of the internet and related activities. The ITE Law set out various terms and definitions relevant for electronic transactions and introduced a number of administrative requirements to conclude digital transactions. The spirit and stated intent of the ITE Law is to protect the state, the public and the private sector against acts of cybercrimes.

The ITE Law stipulates several provisions on personal defamation, online threats and religious blasphemy. In theory, the purpose of these provisions is to enable the arrest and prosecution of cybercriminals. In reality, however, the ITE Law has been used to prosecute individuals for alleged criminal actions online. Provisions of the ITE Law have frequently been used by regional and central government authorities as the legal basis to prosecute citizens who have used the internet to criticise or protest government policies.

As the information technology sector continued to evolve, the Indonesian government sought to keep pace by issuing implementing regulations for the ITE Law and, in 2016, amending the ITE Law itself. With the issuance of Law No. 19 of 2016, the Indonesian government amended several articles in the ITE Law and added a number of new provisions. One of the most controversial amendments was a provision that authorised the government, through the Ministry of Communication and Information (MOCI), to block websites. So, despite the objections of some experts, who argued that blocking websites should only be done by way of a court order, to limit the possibility of any abuse of power, the government is now fully authorised to block websites without any preliminary assessment.

This controversy aside, some parties applauded the ITE Law amendment for providing clearer guidelines on the appropriate use of social media. The Indonesian government seems to have decided to take

a more liberal approach to regulating internet activities, with the expectation that users are able to self-regulate their internet use.

### Legislation

2 | What legislation governs business on the internet?

- Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions or the ITE Law;
- Law No. 8 of 1999 on Consumer Protection (Consumer Protection Law);
- Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (Electronic Transaction Regulation);
- MOCI Regulation No. 36 of 2014 on Procedures for the Registration of Electronic System Providers (MOCI Reg 36/2014);
- MOCI Regulation No. 20 of 2016 on the Protection of Private Data in Electronic Systems (Data Privacy Regulation);
- MOCI Regulation No. 23 of 2013 on the Management of Domain Names (Domain Name Regulation);
- MOCI Regulation No. 19 of 2014 on the Handling of Websites that Contain Negative Content (MOCI Reg 19/2014);
- MOCI Regulation No. 7 of 2016 on the Administration of the Investigation and Prosecution of Criminal Acts in the Field of Information Technology and Electronic Transactions (MOCI Reg 7/2016);
- Ministry of Trade (MOT) Regulation No. 86/M-DAG/PER/12/2016 of 2016 on Requirements for Licensing Services in the Field of E-Commerce Trading and Digital Signatures (MOT Reg 86/2016);
- Ministry of Transportation (MOTR) Regulation No. 108 Of 2017 on the Organization of Non-Fixed Route Public Transportation Services (Transportation Regulation);
- Bank Indonesia (BI) Regulation No. 20/6/PBI/2018 on Electronic Money (E-Money Regulation);
- BI Regulation No. 18/40/PBI/2016 regarding Payment Transaction Processing Operations (BI Reg 18/2016);
- Financial Services Authority (*Otoritas Jasa Keuangan*) (OJK) Regulation No. 77/POJK.01/2016 on Information Technology-Based Money Lending Services (Money Lending Regulation)
- Presidential Regulation No. 74 of 2017 on E-Commerce Roadmap (E-Commerce Roadmap);
- Presidential Regulation No. 44 of 2016 on List of Closed Business Activities and Business Activities Open with Requirements in the Field of Capital Investment (Negative Investment List);
- Chairman of the Capital Investment Coordinating Board (*Badan Koordinasi Penanaman Modal*) (BKPM) Regulation No. 13 of 2017 on Guidelines and Procedures for Capital Investment Licensing and Facilities (BKPM Regulation); and
- MOCI Circular Letter No. 5 of 2016 on Limitations and Liabilities of Platform Providers and Merchants in Conducting Electronic

Commerce in the Form of User-Generated Content (Circular Letter 5/2016).

### Regulatory bodies

- 3 | Which regulatory bodies are responsible for the regulation of e-commerce, data protection and internet access tariffs and charges?

The following regulatory bodies are responsible:

- BI;
- MOCI;
- MOI;
- MOT;
- MOTR; and
- other technical government bodies and institutions relevant to the type of internet-based business.

### Jurisdiction

- 4 | What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions or disputes in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

The ITE Law is applicable to any individual who carries out a certain legal action (as specified in the ITE Law) within or outside Indonesian jurisdiction.

In the event of a dispute, the Indonesian courts shall refer to the ITE Law to determine the competent jurisdiction. For this purpose, the relevant Indonesian court shall use the definition of 'individual' stipulated in the ITE Law, ie, a natural person holding Indonesian or foreign citizenship, which also includes local or foreign legal entities.

Considering that the utilisation of information technology is cross-territorial in nature, it is likely that a foreign citizen or foreign legal entity would be subject to the provisions of the ITE Law to the extent that the concerned legal action had certain legal consequences in Indonesia

### Establishing a business

- 5 | What regulatory and procedural requirements govern the establishment of digital businesses in your jurisdiction? To what extent do these requirements and procedures differ from those governing the establishment of brick-and-mortar businesses?

There are no regulatory and procedural requirements that specifically govern the establishment of digital businesses in Indonesia. The requirements set forth under Law No. 40 of 2007 regarding Limited Liability Companies (Company Law) for establishing a legal entity apply to digital businesses and brick-and-mortar businesses alike.

If the digital business is owned by a foreign individual or body, even if there is no physical presence in Indonesia the business can still be categorised as a permanent establishment (PE). The Indonesian government recently issued Minister of Finance Regulation No. 35/PMK.03/2019 regarding the Determination of Permanent Establishment (MOF Reg 35/2019), which details how to determine whether a foreign individual or body has a PE in Indonesia. If the criteria for a PE are met, the foreign individual or body is required to obtain an Indonesian tax identification number (*Nomor Pokok Wajib Pajak*) (NPWP). In addition, if the foreign individual or body meets the criteria of a taxable entrepreneur for VAT purposes, they must register as a taxable entrepreneur for VAT purposes. In this case, there is no requirement for the foreign individual or body to follow the procedure set forth under the Company Law.

## CONTRACTING ON THE INTERNET

### Contract formation

- 6 | Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

It is possible in Indonesia for parties to agree and enter into a digital agreement. In principle, a digital agreement shall be deemed valid if:

- mutual consent of the parties is accomplished;
- it is concluded by a competent subject of the law or represented according to the prevailing laws and regulations;
- it is executed for a certain matter; and
- the object of the transaction is not prohibited by law, morality or public order.

A digital agreement shall at least contain information on:

- the identity of the parties;
- the object of the agreement and its specifications;
- electronic transaction requirements;
- price and fees;
- the procedure to terminate the agreement;
- a provision that grants a right to the damaged party to receive indemnification for any hidden defect; and
- choice of law to settle the electronic transaction.

Prevailing Indonesian laws and regulations do not specifically address 'click wrap' contracts are whether they are enforceable in Indonesia. Since 'click wrap' contracts are prepared in digital format, such contracts should at least contain the information in the above paragraph to be enforceable. As long as 'click wrap' contracts contain this minimum information, they would be enforceable in Indonesia.

Parties to a digital agreement can use a digital signature. The Indonesian government acknowledges that a digital signature is equally valid as a physical signature. A digital signature shall also be treated as having equal legal force as a physical signature.

### Applicable laws

- 7 | Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

The practice of entering into digital contracts is generally regulated under the Electronic Transaction Regulation. A digital contract can be entered into by a natural person and business entity, either in the form of a legal entity or a non-legal entity. In the private sector, electronic transactions can be concluded among and between:

- businesses;
- businesses and consumers;
- individuals;
- institutions; and
- institutions and businesses in accordance with the applicable laws and regulations.

Nothing in the Electronic Transaction Regulation provides any specific distinction or special treatment if the digital contract is entered into by and between business players.

## Electronic signatures

### 8 | How does the law recognise or define digital or e-signatures?

Indonesia acknowledges digital signatures or e-signatures as a valid signature, regulated by the Electronic Transaction Regulation. Under the Electronic Transaction Regulation, 'digital signature' is defined as a signature comprised of electronic information attached, associated or related to other electronic information used as a tool for verification and validation purposes.

A digital signature shall have a legal binding force to the extent that:

- the data used in forming the digital signature only relates to the signatory;
- the data used in forming the digital signature during the signing process shall only be under the control of the signatory;
- there is a certain method to identify the signatory; and
- there is a method to indicate that the signatory has given his or her consent to the related electronic information.

There are two types of digital signature recognised in Indonesia: certified digital signatures and uncertified digital signatures. A certified digital signature is created by procuring the services of an electronic certification provider and shall be evidenced by an electronic certificate. An uncertified digital signature is created without engaging the services of an electronic certification provider.

## Data retention

### 9 | Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

The implementation of an electronic transaction in Indonesia shall comply with several requirements, one of which is to retain the relevant data domestically. The data of a signatory should be stored in a domestic facility that uses a trustworthy system owned by the digital signature provider and which is able to detect changes to the information. A trustworthy system shall be regarded as a system that follows procedure for the utilisation of a digital signature that confirms its genuineness and the integrity of the electronic information.

In addition to the obligation to retain the data domestically, electronic system providers shall guarantee that their software does not contain any unusual or hidden instructions that can be construed as a violation of the law. For example, an instruction to detonate a time bomb, virus, Trojan horse, worm or backdoor.

Electronic system providers that retain source code escrow, in cooperation with trusted third parties, shall take reasonable efforts to mitigate these occurrences by checking the source code.

## Breach

### 10 | Are any special remedies available for the breach of electronic contracts?

The Indonesian Consumer Protection Law and the ITE Law provide that a consumer can file a lawsuit if an electronic system provider does not fulfil its obligations. In addition to settling disputes through the Indonesian courts or through alternative dispute resolution mechanisms, consumers can file a claim with the Consumer Dispute Settlement Board (BPSK). The BPSK was established through the enactment of the Consumer Protection Law.

## SECURITY

### Security measures

#### 11 | What measures must be taken by companies or ISPs to guarantee the security of internet transactions? Is encryption mandatory?

By regulation, an electronic system provider is obligated to guarantee the security of the software used to facilitate and administer the electronic system services, as well as to assure that an information security agreement is available. In practice, an electronic system provider is required to establish a security system that has a system and procedure for countermeasures and prevention of threats and attacks that could lead to disruptions, failure and financial loss for users.

### Government intervention and certification authorities

#### 12 | As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

The government is obligated to prevent the distribution and use of electronic information or documents that contain prohibited materials pursuant to the prevailing laws and regulations. To prevent such distribution and use, the government is authorised to cut access or have electronic system providers cut off access to any electronic information or document that contains prohibited materials.

The ITE Law also recognises that government officials have certain authorities to investigate criminal acts or potential criminal acts in the field of electronic transactions and information. Such authorities include:

- receiving reports on criminal acts in the field of electronic transactions and information;
- summoning the relevant parties for further investigation;
- investigating the facts related to reports of alleged criminal acts;
- investigating the party that is claimed to have committed the alleged criminal act;
- examining the tools used in performing the alleged criminal act;
- searching certain locations where the alleged criminal act was committed;
- confiscating the tools used to perform the alleged criminal act;
- causing electronic information or data related to the criminal act to be inaccessible;
- requesting information in the electronic system or information produced by the electronic system that is relevant to the criminal act;
- requesting experts as necessary to carry on with the investigation of the criminal act.

## Electronic payments

#### 13 | Are there any rules, restrictions or other relevant considerations regarding the use of electronic payment systems in your jurisdiction?

MOCI strictly requires electronic system providers, including those that facilitate electronic payment systems, to register with it. Electronic system providers that facilitate the use of electronic payment systems, including e-wallets, must also obtain a license from Indonesian's central bank, BI.

#### 14 | Are there any rules or restrictions on the use of digital currencies?

BI regulates that digital currencies, including Bitcoin, are not considered a valid payment instrument. Therefore, the use of digital currency as a payment instrument is restricted in Indonesia. BI further emphasises that payment system services and financial technology providers are restricted from processing payment transactions that use digital currency.

### DOMAIN NAMES

#### Registration procedures

#### 15 | What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

Registration of a domain name is administered on a first-come, first-served basis. The process, which is straightforward, is initiated by the domain name user submitting an application along with the required supporting documents to the domain name registrar. The domain name registration process shall not take more than five business days after a completed domain name registration is submitted and received by the domain name organiser. A non-resident can file a domain name registration application after going through the evaluation process to confirm that the foreign application complies with the administrative and financial requirements to be eligible for an Indonesian domain name.

#### Rights

#### 16 | Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

There are no additional rights vested to domain name users, except for the right of domain name users to transfer the domain name registration to another domain name user.

#### Trademark ownership

#### 17 | Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

According to the Domain Name Regulation, an international holder of a trademark that has been registered in Indonesia is entitled to register, use, and benefit from the Indonesian domain name. The registration of a domain name by such international trademarked organisation shall be done through an Indonesian entity by way of power of attorney.

The Domain Name Regulation does not require submission of a trademark license to register a domain name. Although that is the case, in practice, valid evidence of trademark ownership is helpful as a supporting document when a registrar receives two applications for registration that contain similar domain names. Submitting such a trademark licence is also helpful in deciding which of the two applications will be deemed a 'pirate' registration.

#### Dispute resolution

#### 18 | How are domain name disputes resolved in your jurisdiction?

Domain name disputes in Indonesia should be settled through the Indonesian Internet Domain Name Administrator (PANDI), which derives its authority to settle such disputes from the Domain Name Dispute Resolution (PPND). The Electronic Transaction Regulation defines 'domain dispute' as a situation in which one party's rights to a registered domain name have been breached by another party. However, this does not include disputes involving the content of a domain or the

management of domain names. In other words, not all domain name disputes can be settled through PANDI.

### ADVERTISING

#### Regulation

#### 19 | What rules govern advertising on the internet?

There is no specific rule that governs online advertising activities. Considering that online advertising is part of an electronic transaction, such advertising is subject to the provisions of the ITE Law, the Electronic Transaction Regulation and other relevant regulations on internet-based activities.

In relation to capital investment restrictions, the Negative Investment List stipulates that activities concluded using an electronic system, including online-based ads, are subject to a maximum 49 per cent foreign ownership if the investment value is less than 100 billion rupiah.

The Electronic Transaction Regulation only provides that an electronic system provider shall formulate a feature for the purpose of accessing information regarding advertisements.

#### Definition

#### 20 | How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

There is no specific definition of 'online advertising' provided in the applicable laws and regulations in Indonesia, because online advertising is deemed an inseparable part of an electronic transaction. Online advertising activity is useful for merchants to introduce and promote their products and services. However, there are also companies established with the sole purpose to conduct online advertising services. These companies profit by designing advertisement materials, distributing those materials to numerous platforms and arranging for the ads to be published. It is unlikely for online editorial content to be classified as online advertising, since online editorial content may not necessarily be intended for commercial purposes.

#### Misleading advertising

#### 21 | Are there rules against misleading online advertising?

The Consumer Protection Law provides that any business entity that uses misleading information for online advertisement purposes shall be subject to imprisonment for a maximum period of five years or financial penalties in a maximum nominal value of 2 billion rupiah.

#### Restrictions

#### 22 | Are there any products or services that may not be advertised on the internet?

According to the applicable laws and regulations, products or services which are prohibited to be advertised or distributed through the internet include obscene content, gambling-related content, defamatory material, and blackmail-related content.

#### Hosting liability

#### 23 | What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

If the content providers merely host the content, then their liability would be limited to the information indicated within the relevant content. If the content is unlawful, but remains unpublished, then the

content providers will be solely liable. However, if such unlawful content is published on a website, the relevant internet system provider can also be held liable, if it cannot prove that its system is not classified as a user-generated electronic system. If it is published in a non-user generated electronic system, the internet system provider would have control to decide whether the content is lawful before publishing.

## FINANCIAL SERVICES

### Regulation

**24** | Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

No specific regulation on the advertisement or selling of financial services products has been issued by the Indonesian government. Hence, this topic is covered under the ITE Law and its implementing regulations.

## DEFAMATION

### ISP liability

**25** | Are ISPs liable for content displayed on their sites? How can ISPs limit or exclude liability?

As a general rule, an electronic system provider must maintain a reliable and secure electronic system. Under the ITE Law, an electronic system provider shall be held responsible for the operation of its electronic system. However, in practice, it is difficult for system providers to entirely supervise the content displayed on websites, especially if it involves a user-generated electronic system. In order to address this issue, MOCI issued Circular Letter 5/2016, which provides that although providers are to be held responsible for the organisation of their platforms, said providers will no longer be held liable if they can prove that the disadvantageous action in question on their platforms was caused by users.

In order to limit or exclude liability, electronic system providers that have user-generated content should comply with the obligation to provide terms and conditions for the platform. These terms and conditions should at least contain the obligations and rights of users in regard to uploaded content. By clearly stipulating that users are responsible for their uploaded content, electronic system providers can limit or exclude liability for the content displayed on their platforms.

### Shutdown and takedown

**26** | Can an ISP shut down a web page containing defamatory material without court authorisation?

The system provider is under the obligation to have a mechanism to delete electronic information that becomes irrelevant in accordance with the prevailing laws and regulations. Initially, the ITE Law provided that a system provider could only delete certain content based on a court order. The government seems to have removed the requirement to obtain a court order through the issuance of Circular Letter 5/2016. The system provider is now required to delete or block any defamatory material after it receives a report on the existence of such material.

Further, governmental institutions, law enforcers, and the general public may submit a report to MOCI so that specific websites may be blocked due to unlawful content. Upon receiving a report, MOCI will add the reported website to the TRUST+ Positive list, which is a database of websites with negative content. Internet service providers must block access to all websites on the TRUST+ Positive list. Such blocking can be performed independently by the internet service provider itself or

through a blocking service provider. Internet service providers that fail to block websites on the TRUST+ Positive list may be subject to criminal and administrative sanctions.

## INTELLECTUAL PROPERTY

### Third-party links, content and licences

**27** | Can a website owner link to third-party websites without permission?

Based on Indonesian laws and regulations, a website shall be regarded as an intellectual property of the system provider that has gathered the electronic information and documents to establish the website. In theory, a website owner has no IP rights over the content displayed by another provider. If one intends to insert a link to access a third party's website, then permission from the operator of such website is advisable even if the content of such a third party's website does not contain materials that may violate the applicable laws and regulations.

**28** | Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?

In practice, many website owners use content owned by other website owners without permission. As long as the relevant content is used for lawful purposes, the potential consequence would only be civil in nature. However, if the content has indications of, for example, gambling activities, then it could be subject to criminal sanctions.

**29** | Can a website owner exploit the software used for a website by licensing the software to third parties?

There is no restriction on a website owner or an electronic system provider cooperating with third parties for the purpose of exploiting software. However, it is important to note that the website owner should first confirm whether the relevant third parties are trustworthy, because a website owner is under the obligation to protect the confidentiality of source code attached to the software.

**30** | Are any liabilities incurred by links to third-party websites?

If links to third-party websites are displayed, then the relevant owner of the website would automatically be liable for the content of such third-party website. The owner of the website will not be liable if there is an agreement among the website owners that contains a provision that the original website owner shall be liable for any transmission of the content used on its website.

### Video content

**31** | Is video content online regulated in the same way as TV content or is there a separate regime?

Video content accessible through a website is regulated under the same regime as other forms of electronic information or document, since the definition of electronic information or document in the ITE Law is very broad. As such, there is no special treatment or exemption for video content that is available online and publicly accessible.

## IP rights enforcement and remedies

32 | Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

With the issuance of MOCI Reg 7/2016, the relevant authorities are only able to carry out dawn raids and conduct an arrest if the actions are considered as criminal activities under the electronic information technology regime. As to intellectual property infringement, the most aggressive sanction that can be imposed is the suspension of the provider's website for a certain period of time.

33 | What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

See question 32.

## DATA PROTECTION AND PRIVACY

### Definition of 'personal data'

34 | How does the law in your jurisdiction define 'personal data'?

The Data Privacy Regulation defines personal data as certain individual data, the authenticity of which is verified, sustained and maintained while its confidentiality remains protected.

### Registration requirements

35 | Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?

Any personal data may only be utilised within the certified electronic system and it must at all times be protected during the implementation of the personal data management activities.

### Cross-border issues

36 | Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?

Any transfers of personal data from a domestic organiser to a foreign country must be coordinated via MOCI in accordance with the prevailing laws and regulations for cross-border exchanges of personal data.

### Customer consent

37 | Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?

Personal data can be managed by an organiser based on a written consent of the owner. By maintaining such consent, an organiser is entitled to legally undertake the receipt, collection, processing, analysis, saving, display, announcement, transmission, dissemination, opening of access and deletion of such personal data.

### Sale of data to third parties

38 | May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?

Indonesian legislation does not recognise personal data as a commodity that can be used for trading purposes. By definition, the ownership of personal data will always be attached to the relevant individual. In theory,

however, if the individual has consented to his or her personal data being transferred, that particular transfer should be deemed as lawful.

### Customer profiling

39 | If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?

There is no specific rule regarding technical activities that relate to personal data in Indonesia. However, the profiling of customers to be used for targeted advertising by a website owner would still be lawful if the website owner upholds the confidentiality principles adopted by the Data Privacy Regulation.

### Data breach and cybersecurity

40 | Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?

The Data Privacy Regulation provides that in case of a failure to keep personal data confidential, the relevant electronic system provider shall notify the owner of the personal data within a maximum of 14 days as of the date such failure becomes known to the provider.

41 | What precautionary measures should be taken to avoid data breaches and ensure cybersecurity?

In terms of Indonesian regulation, there are no specific requirements or guidelines that electronic system providers must follow to avoid data breaches and ensure cybersecurity. If an electronic system provider wants to help ensure cybersecurity, it can retain the services of competent professionals. In Indonesia, information security consulting services are listed in the Indonesia Standard Industrial Classification (*Klasifikasi Baku Lapangan Usaha Indonesia*) (KBLI), which classifies the different business activities and fields in Indonesia.

### Insurance

42 | Is cybersecurity insurance available and commonly purchased?

Cybersecurity insurance is available in Indonesia but it is not commonly purchased. Most insurance companies view that it is difficult to sell cybersecurity insurance because of the low rate of cybercrime and data breaches in Indonesia.

### Right to be forgotten

43 | Does your jurisdiction recognise or regulate the 'right to be forgotten'?

Indonesia recognised the 'right to be forgotten' in 2016 through the issuance of an amendment to the ITE Law. Only the relevant user can submit an application to erase electronic information or document, and the application to shall be addressed to the relevant competent court.

Electronic system providers must provide a mechanism to erase electronic information or documents, and they shall erase the concerned electronic information or documents upon receiving a court order.

### Email marketing

44 | What regulations and guidance are there for email and other distance marketing?

Indonesia does not have any specific rules on email. The definition of 'electronic information' provided in the ITE Law includes 'email'.

## Consumer rights

- 45 | What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

The individuals who own the personal data have the right to report the failure to process their personal data. The right to file a report is intended to allow negotiations between the parties to reach an amicable agreement. The Data Privacy Regulation is silent on whether 'owner of personal data' includes foreign citizens.

## TAXATION

### Online sales

- 46 | Is the sale of online products subject to taxation?

Yes, the sale of online products is subject to taxation. Indonesian law does not specify any tax exemption for the sale of products through online systems.

### Server placement

- 47 | What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

An operator shall be treated as a resident taxpayer and subject to local tax laws in the jurisdiction where the server is placed, provided that the tax treaty signed between the relevant countries indicates that the placement of a server constitutes a permanent establishment.

### Company registration

- 48 | When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

Companies classified as taxable entrepreneurs (ie, they have annual sales revenue greater than 4.8 billion rupiahs) must pay and report VAT by way of e-filing at the end of each month. Indonesian tax laws provide no special treatment or exemption to the imposition of applicable taxes for transactions concluded online (see question 39). Hence, transactions concluded through an online system are subject to VAT and income tax.

### Returns

- 49 | If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

Assuming that the goods are imported from an offshore company to Indonesia, they will be subject to import duty. If those goods are returned to the offshore company, they will be considered as exports, which are subject to VAT of zero per cent.

If the offshore company delivers the goods directly to Indonesian customers, there should be no VAT payable to the local entity, in which case the local entity will not pay VAT to the offshore entity for obtaining the goods. Consequently, the onshore company is not obligated to file a monthly VAT report with the tax office.

We do not foresee any transfer pricing problems, provided that the offshore and onshore companies do not have any special relationship. A special relationship is deemed to exist in the following circumstances, pursuant to article 18(4) of Law No. 36 of 2006 on Income Tax (the Income Tax Law):

- where a taxpayer directly or indirectly holds 25 per cent or more of the capital of another taxpayer, or where a company holds 25 per cent or more of the capital of two taxpayers, in which case the latter two taxpayers are also considered to be related parties;
- where there is control through management or the use of technology, even if an ownership relationship is not present; or
- where there is a family relationship, either through blood or through marriage within one degree of direct or indirect lineage.

## GAMBLING

### Legality

- 50 | Is it permissible to operate an online betting or gaming business from the jurisdiction?

It is not permitted as gambling is strictly prohibited under the applicable Indonesian laws and regulations.

- 51 | Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Since the ITE Law applies cross-border to jurisdictions all over the world, a resident would be prohibited to participate in online casinos and betting websites.

## OUTSOURCING

### Key legal and tax issues

- 52 | What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

There are only certain services or activities, considered as non-core activities, that can be outsourced to other companies. If an outsourcing arrangement is put in place for core business activities, the outsourcing agreement will be deemed null and void.

### Employee rights

- 53 | What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, and do the rules apply to all employees within the jurisdiction?

The employees who have been replaced by way of termination due to their positions being outsourced shall be entitled to termination benefits.

## ONLINE PUBLISHING

### Content liability

- 54 | When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability? Is it required or advised to post any notices in this regard?

A website provider shall be held liable for the information it provides online if that information is found to be false. The website provider can avoid such liability if it can prove that its system is user generated. To exclude liability, the website provider should inform users that they are accessing a user-generated platform and that the users shall be liable for any information they provide online. For practical purposes, the website provider can simply provide a standard agreement form that sets out that users shall be responsible for any information they provide online.

There is no specific requirement for the provider to post any notice in this regard, except in the event of data breach or failure to protect the confidentiality of personal data. The electronic system provider must provide a notification to the data subject with the reason or cause of the failure to protect the confidentiality of the personal data. The notification may be sent electronically if the data subject approved such electronic notification during the acquisition and collection of their personal data. The electronic system provider must ensure that the notification has been received by the data subject if the data breach has the potential to cause loss to the relevant data subject. The electronically transmitted notification must be sent to the data subject no later than 14 days after the identification of the breach. In addition, although there is no legal requirement to notify the government of such a data breach, MOCI has verbally stated on multiple occasions that it expects an electronic system provider to notify it of any data breach, but that failing to do so will not result in any sanction.

### Databases

**55** | If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

A database should be fully controlled by the website provider. One of the obligations of a website agent provider is to confirm the control over authorisation and access rights to the database and the electronic transaction.

## DISPUTE RESOLUTION

### Venues

**56** | Are there any specialist courts or other venues in your jurisdiction that deal with online/digital issues and disputes?

There is no special court or venue to resolve online/digital disputes in Indonesia. Principally, the method to settle an online/digital dispute should be agreed by both parties in their digital agreement. However, if the dispute involves personal data, MOCI may delegate its authority to the Director General of Informatics Application (Director General), who will form a data privacy dispute settlement panel. This panel may provide a recommendation to MOCI to impose administrative sanctions against the relevant electronic system provider, although the dispute can also be settled amicably or by any other alternative dispute resolution process between the electronic system provider and the owner of the data.

### ADR

**57** | What alternative dispute resolution (ADR) methods are available for online/digital disputes? How common is ADR for online/digital disputes in your jurisdiction?

The parties are free to determine an alternative dispute resolution method. There is no legal requirement in Indonesian law to choose a certain ADR method. For online/digital disputes, we have found that mediation and arbitration are the most common methods of dispute settlement in Indonesia.



#### Fahrul S Yusuf

fahrulyusuf@ssek.com

#### Mohammad K Bratawijaya

mohammadbratawijaya@ssek.com

14th floor, Mayapada Tower I

Jl Jend Sudirman Kav 28

Jakarta 12920

Indonesia

Tel: +62 21 521 2038

Fax: +62 21 521 2039

www.ssek.com

## UPDATE AND TRENDS

### Key developments of the past year

**58** | Are there any emerging trends or hot topics in e-commerce regulation in the jurisdiction? Is there any pending legislation that is likely to have consequences for e-commerce and internet-related business?

The Indonesian House of Representatives is said to be in the process of discussing a draft law on personal data protection (PDP Draft Law). Based on media reports, the PDP Draft Law is on track to be issued by the end of 2019. If enacted, the PDP Draft Law would be the first comprehensive law in Indonesia to specifically deal with the protection of personal data. The current draft seems to include several provisions similar to those found in various jurisdictions that give individuals more control of their online information.

There has also been an effort to amend the Electronic Transaction Regulation (GR 82 Draft Amendment). It appears that the GR 82 Draft Amendment introduces several categories of data that do not exist in the Electronic Transaction Regulation, such as strategic electronic data, high-risk electronic data and low-risk electronic data, all of which would trigger different levels of responsibility for the electronic system provider.

The two aforementioned drafts are 'live' drafts and subject to further change. Therefore, it cannot be guaranteed that the changes discussed above will be included in the final drafts.

## Other titles available in this series

Acquisition Finance	Distribution & Agency	Islamic Finance & Markets	Real Estate M&A
Advertising & Marketing	Domains & Domain Names	Joint Ventures	Renewable Energy
Agribusiness	Dominance	Labour & Employment	Restructuring & Insolvency
Air Transport	e-Commerce	Legal Privilege & Professional Secrecy	Right of Publicity
Anti-Corruption Regulation	Electricity Regulation	Licensing	Risk & Compliance Management
Anti-Money Laundering	Energy Disputes	Life Sciences	Securities Finance
Appeals	Enforcement of Foreign Judgments	Litigation Funding	Securities Litigation
Arbitration	Environment & Climate Regulation	Loans & Secured Financing	Shareholder Activism & Engagement
Art Law	Equity Derivatives	M&A Litigation	Ship Finance
Asset Recovery	Executive Compensation & Employee Benefits	Mediation	Shipbuilding
Automotive	Financial Services Compliance	Merger Control	Shipping
Aviation Finance & Leasing	Financial Services Litigation	Mining	Sovereign Immunity
Aviation Liability	Fintech	Oil Regulation	Sports Law
Banking Regulation	Foreign Investment Review	Patents	State Aid
Cartel Regulation	Franchise	Pensions & Retirement Plans	Structured Finance & Securitisation
Class Actions	Fund Management	Pharmaceutical Antitrust	Tax Controversy
Cloud Computing	Gaming	Ports & Terminals	Tax on Inbound Investment
Commercial Contracts	Gas Regulation	Private Antitrust Litigation	Technology M&A
Competition Compliance	Government Investigations	Private Banking & Wealth Management	Telecoms & Media
Complex Commercial Litigation	Government Relations	Private Client	Trade & Customs
Construction	Healthcare Enforcement & Litigation	Private Equity	Trademarks
Copyright	High-Yield Debt	Private M&A	Transfer Pricing
Corporate Governance	Initial Public Offerings	Product Liability	Vertical Agreements
Corporate Immigration	Insurance & Reinsurance	Product Recall	
Corporate Reorganisations	Insurance Litigation	Project Finance	
Cybersecurity	Intellectual Property & Antitrust	Public M&A	
Data Protection & Privacy	Investment Treaty Arbitration	Public Procurement	
Debt Capital Markets		Public-Private Partnerships	
Defence & Security		Rail Transport	
Procurement		Real Estate	
Dispute Resolution			

Also available digitally

[lexology.com/gtdt](https://www.lexology.com/gtdt)