Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

Malaysia: Law and Practice & Trends and Developments

Janet Toh, Irene Yong, Krystle Lui, Boo Cheng Xuan and Yee Yong Xuan
Shearn Delamore & Co.

MALAYSIA

Law and Practice

Contributed by:
Janet Toh, Irene Yong, Krystle Lui and Boo Cheng Xuan
Shearn Delamore & Co.

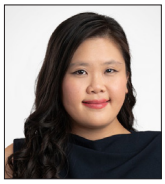
Contents

Shearn Delamore & Co. was established in 1905, and is one of the leading and largest law firms in Malaysia. With over 120 lawyers and 230 staff, the firm has the resources to run and manage the most complex projects, transactions and matters. The firm maintains extensive global network links with foreign law firms and multilateral agencies, and is a founding member of the blue-chip legal network Drew Network Asia (DNA). The firm's technology, multimedia and telecommunications practice group, comprising lawyers from various disciplines including IP, financial services, corporate and M&A, tax and competition, assists clients with the legal issues emerging from the convergence of technology, media and communications. It provides clients with comprehensive and practical legal solutions tailored for an increasingly digital world. The approach and solutions are tailored to meet clients' specific strategic and commercial objectives.

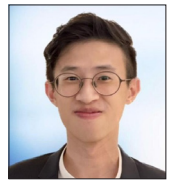
Authors

Janet Toh has over 20 years of experience in intellectual property and technology law. She co-heads the technology, multimedia and telecommunications practice group and leads the personal data protection practice group at Shearn Delamore & Co. Janet advises on IP protection, advertising, e-commerce, franchising, gaming, regulatory approvals and telecommunications. She handles technology and commercial transactions, including outsourcing, software licensing, and IT system development across industries. Janet also counsels clients on data protection, privacy and cybersecurity. She is the deputy chairperson of the Bar Council Cyber and Privacy Law Committee and a member of ITechLaw.

Irene Yong is a partner at Shearn Delamore & Co. She practises in all aspects of tax and revenue law advisory, structuring, planning, audits, investigations, dispute resolution and tax litigation (including tax appeals, declaratory proceedings, judicial review applications, civil suits, windings up etc.). She has appeared as counsel for taxpayers before the Customs Appeal Tribunal, GST Appeal Tribunal, Special Commissioners of Income Tax and the Superior Courts of Malaysia. She also practises in the area of personal data protection and privacy laws, and has advised and conducted reviews and audits for various business enterprises apart from regularly conducting PDPA training and workshops.



Krystle Lui is a partner at Shearn Delamore & Co. where she provides legal advice on laws regulating financial services and institutions, and capital market services and intermediaries to both foreign and local clients. She also has niche experience in advising on Islamic structures, derivatives, collective investment schemes, payment systems and payment instruments. Examples include advising foreign institutions on reach-in and onshore activities relating to offerings of securities and digital assets in Malaysia, drafting terms and conditions for the banking services of a new digital bank, and advising on the regulation of payment systems and electronic trading platforms.



Boo Cheng Xuan is part of the technology, multimedia and telecommunications practice group at Shearn Delamore & Co. He focuses on advisory and transactional matters related to digital technology and cybersecurity, including digital banking, fintech, the metaverse, AI, data centres, cloud computing, telecommunications, software, e-commerce and gaming. He also assists clients in responding to cyber-attacks and data breaches. Cheng Xuan is a member of the Malaysian Bar's National Young Lawyers and Pupils Committee, LAWSIA's Communications, Technology and Data Protection Committee, and LAWASIA's Emerging Lawyers Committee. He has spoken on and moderated discussions about legal technology at the Taiwan-Malaysia Young Lawyers Forum 2023 and the Malaysia-Singapore Young Lawyers' Summit 2024.

Shearn Delamore & Co.

7th Floor, Wisma Hamzah-Kwong Hing
No 1 Leboh Ampang
50100 Kuala Lumpur
Malaysia

Tel: +60 3 2027 2727
Fax: +60 3 2078 5625
Email: info@@shearndelamore.com
Web: www.shearndelamore.com

Shearn Delamore &CO.

1. Digital Economy

1.1 Key Challenges

In Malaysia, the digital economy is not governed by a single legal framework. Instead, its regulation spans various statutes, subsidiary legislation, case laws, guidelines and industry codes relating to matters such as data protection, communications, media, consumer protection, electronic transactions and cybersecurity, some of which are discussed below.

The Electronic Commerce Act

The Electronic Commerce Act 2006 (ECA), which aims to enable and facilitate commercial transactions through the use of electronic means, effectively serves as a statutory recognition of contracts formed by electronic means. It provides that a contract shall not be denied legal effect, validity or enforceability on the ground that an electronic message is used in its formation.

Communications and Multimedia Act

Online communications and contents play a significant role in the digital economy. In this regard, communications are primarily regulated by the Communications and Multimedia Act 1998 (CMA). The CMA provides for, among others, the regulation of content, and the licensing of providers of network facilities, network services, applications services and content applications services. Services such as internet access, cloud, social media, messaging (including internet messaging) – all of which are intrinsically linked to the digital economy, would fall within the purview of the CMA.

The CMA prohibits certain types of content and communications, such as indecent and offensive content and communications, which would limit the types of digital activities and services that can be offered or conducted within the digital economy. Content is also regulated through the Malaysian Communications and Multimedia Content Code (Third Edition, 2022) (the "Content Code"), issued and administered by the Communications and Multimedia Content Forum of Malaysia (the "Content Forum"), and registered as a voluntary industry code under the CMA. This means that, unless otherwise subject to any direction by the Malaysian Communications and Multimedia Commission to comply with it, compliance with the Content Code is voluntary.

However, compliance with the Content Code shall be a defence against any prosecution, action or proceeding of any nature. In this connection, the Content Code provides guidelines on various types of contents including online contents and advertisements.

Other Legislation

Other relevant legislation includes the Penal Code, Financial Services Act 2013, the Consumer Protection Act 1999 (CPA) including the Consumer Protection (Electronic Trade Transactions) Regulations 2012 (CPETTR), Strategic Trade Act 2010, Computer Crimes Act 1997, Digital Signature Act 1997, and Copyright Act 1987.

Challenges

As the internet serves as the backbone for most activities within the digital economy, the inherent reliance on the internet brings about significant challenges, particularly in the realm of cybersecurity and data protection, where vulnerabilities to hacking, data breaches and cyber-attacks pose risks to businesses and consumers alike. Additionally, the vast amount of data generated, collected and processed raises critical concerns regarding data protection and privacy, especially when data flows across jurisdictions and may end up at a place without adequate legal protec-

tion. In an effort to address these challenges, the Cyber Security Act 2024 (CSA) was recently introduced, followed by amendments to the Personal Data Protection Act 2010 (PDPA).

CSA

The CSA came into force on 26 August 2024 alongside subsidiary regulations relating to the notification of cybersecurity incidents, risk assessments, licensing of cybersecurity service providers, etc. Public and private entities (including private businesses) that are designated as national critical information infrastructure entities ("NCII Entities") and cybersecurity service providers will be expected to comply with the regulatory requirements under the CSA and the above-mentioned regulations.

One of the main focuses of the CSA is the protection of national critical information infrastructure (NCII), defined to mean a "computer or computer system which the disruption to or destruction of the computer or computer system would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the state governments to carry out its functions effectively". The CSA identifies the following 11 sectors as NCII sectors, and any person or entity operating within such sectors may potentially be designated as an NCII Entity if the relevant sector lead tasked to carry out the designation is satisfied that such person or entity owns or operates an NCII:

- government;
- banking and finance;
- transportation;
- defence and national security;
- information, communication and digital;
- healthcare services;
- water sewerage and waste management;
- energy;
- agriculture and plantation;
- trade, industry and economy; and
- science, technology and innovation.

The CSA imposes various duties on an NCII Entity, including those relating to the implementation of measures, standards and processes, cybersecurity risk assessments, cybersecurity audits and notification of cybersecurity incidents.

PDPA

Where processing of personal data in commercial transactions is involved, the PDPA, which is the primary legislation governing the processing of personal data, will apply. The PDPA requires, among others, compliance with the seven Personal Data Protection Principles, namely the General Principle, the Notice and Choice Principle, the Disclosure Principle, the Security Principle, the Retention Principle, the Data Integrity Principle, and the Access Principle, as well as other requirements such as those for the cross-border transfer of personal data.

Amendments to the PDPA pursuant to the Personal Data Protection (Amendment) Act 2024 (the "PDP Amendment Act") aim to strengthen the data protection framework, including the introduction of data processors' obligations, data portability rights, the requirement to a appoint data protection officer and mandatory data breach notifications, and they are being implemented in phases over the first half of 2025. This means that businesses that process personal data, including those in the digital economy sector, will have to adapt their business operations to align with the amended PDPA requirements. These adjustments may include reviewing data processing practices, updating internal policies, enhancing data security meas-

ures, and ensuring adequate training for personnel to meet the new legal standards.

The advent of digital economy also brings about concerns on online safety, which is sought to be addressed by the Online Safety Bill 2024 (OSB). The OSB seeks to enhance and promote online safety and regulate harmful content by providing for duties and obligations of the applications service providers (ASPs), content applications service providers (CASPs) and network service providers, while strengthening regulatory oversight in the digital space. Upon receiving Royal Assent and being gazetted, the OSB will take effect on a date specified by the Minister of Communications.

1.2 Digital Economy Taxation

Service Tax

For purposes of the Service Tax Act 2018 (STA), "digital service" refers to "any service that is delivered or subscribed over the internet or other electronic network and which cannot be obtained without the use of information technology and where the delivery of the service is essentially automated".

"Digital service" is prescribed as a taxable service, meaning that 8% service tax is chargeable under the STA upon any digital service provided in Malaysia by a registered person in carrying on their business.

"Digital service" also includes the provision of an electronic medium that allows suppliers to provide supplies to customers or transactions for provision of digital services on behalf of any person.

The service provider will be required to be registered under the STA and charge service tax if the total value of its taxable services in a particular month and the 11 months immediately preceding that month has exceeded MYR500,000 or, where there are reasonable grounds for believing that the total value of all its taxable services in that month and the 11 months immediately succeeding that month will exceed MYR500,000, whichever is earlier.

Imported digital services are also subject to the 8% service tax on digital services acquired by any person in Malaysia from any person who is outside Malaysia in B2B transactions. The recipient of the imported services must account for and pay the service tax to the Royal Malaysian Customs Department ("Customs").

The 8% service tax is also applicable where a foreign service provider provides any digital service to consumers. "Consumer" means any person who fulfils any two of the following:

- makes payment for digital services using credit or debit facility provided by any financial institution or company in Malaysia;
- acquires digital services using an internet protocol address registered in Malaysia or an international mobile phone country code assigned to Malaysia; or
- resides in Malaysia.

Such foreign service providers will be required to register under the STA within the stipulated period if the total value of all its digital services to consumers in a particular month and the 11 months immediately preceding that month has exceeded MYR500,000 or where there are reasonable grounds to believe that the total value of all its digital services in the next 12 months will exceed MYR500,000, whichever is earlier. They will also have to file the relevant service tax returns and account for the service tax to Customs, among other reporting obligations.

Digital services provided in relation to matters outside Malaysia are exempt from service tax as are those provided by a company to any company within the same group of companies provided certain conditions are met.

Withholding Tax

A 10% withholding tax (subject to any exemption or reduced tax rate available under the applicable double tax treaty (DTA)) is also levied on payments to a non-resident in consideration of any advice given, or assistance or services rendered, in connection with the management or administration of any scientific, industrial or commercial undertaking, venture, project or scheme which are derived or deemed derived from Malaysia. However, no withholding tax applies if such technical advice, assistance or services are rendered outside of Malaysia.

Where the provision of the digital service or product involves a royalty payment, withholding tax obligations may arise upon the payment of "royalties" derived from Malaysia to a non-resident person (unless attributable to a business of the non-resident carried on in Malaysia). The payer must deduct and withhold tax at 10% of the gross amount (subject to any exemption or reduced tax rate available under the applicable DTA).

Royalties would be deemed to be derived from Malaysia if, among other things, responsibility for payment lies with a person who is tax-resident in Malaysia for that basis year.

"Royalty" is given a very broad definition under the Income Tax Act 1967 (ITA), being deemed to include any sums paid as consideration for, or derived from:

- the use of, or the right to use in respect of, any copyrights, software, artistic or scientific works, patents, designs or models, plans, secret processes or formulae, trade marks or other like property or rights;
- the use of, or the right to use, know-how or information concerning technical, industrial, commercial or scientific knowledge, experience or skill;
- the alienation of any property, know-how or information mentioned in the foregoing paragraphs.

Where a DTA has been concluded between Malaysia and the jurisdiction in which the non-resident is tax-resident, the treaty provisions will prevail over the ITA in the event of a conflict. That is to say, the treaty definition of "royalty" will apply in such circumstances rather than the broad definition of the same under the ITA so that the payment in question may not be subject to Malaysian withholding tax.

Challenges

One of the challenges is the differing views which the payer and service provider may take with regard the characterisation of the payment as royalty or a payment for services.

As the withholding tax liability (if any) is imposed upon the payer, some payers may subject payment of the fees for such digital services or goods to withholding tax since the Malaysian Inland Revenue Board is likely to regard payments relating to software as constituting royalty and will penalise the payer if the payments to the non-resident are not subjected to withholding tax.

As such, parties should ensure that the contracts are clearly drafted and indicate who should bear the withholding tax, in the event it is applicable.

1.3 Taxation of Digital Advertising

Advertising service, including digital advertising, is prescribed as a taxable service, meaning that, 8% service tax is chargeable under the STA upon any advertising service provided in Malaysia by a registered person in carrying on their business.

Similarly, imported advertising services are also subject to the 8% service tax if such services are acquired by any person in Malaysia from any person who is outside Malaysia in B2B transactions. The recipient of the imported services must account for and pay the service tax to Customs.

The 8% service tax is also applicable where a foreign service provider provides any digital service to consumers, as explained in **1.2 Digital Economy Taxation**.

Service tax is not chargeable on advertising services provided for promotion outside Malaysia or on advertising services provided by a company to any company within the same group of companies if the relevant conditions are met.

A 10% withholding tax may also apply, as discussed in **1.2 Digital Economy Taxation**. However, no withholding tax applies if the advertising services were wholly rendered outside of Malaysia.

1.4 Consumer Protection

The CPA is the key legislation governing consumer rights in Malaysia, including those relevant to digital goods and services. Although not drafted with online transactions in mind, its scope has expanded to cover online transactions, particularly after the introduction of the CPETTR. Key features of the CPA include protections against misleading conduct, false representations and unfair practices, along with guarantees for acceptable quality, fitness for purpose, and the right to redress.

The CPETTR in turn requires the supply of goods and services through websites or online marketplaces to be accompanied by disclosure of mandatory information such as the full price of the goods or services including transportation costs, taxes and any other cost, and mandates online marketplace operators to maintain records of the sellers and service providers trading on their platform. These provisions ensure comprehensive consumer protection in the evolving digital economy.

Please note that other laws such as the Sale of Goods Act 1957, Contracts Act 1950, Trade Descriptions Act 2011 and the Price Control and Anti-Profiteering Act 2011 also contain provisions that may be relevant to consumer protection within the digital economy.

1.5 The Role of Blockchain in the Digital Economy

The Securities Commission Malaysia (SC) is the primary regulator of the digital asset industry in Malaysia and has developed a regulatory framework that treats certain digital currencies and digital tokens as securities for the purposes of securities law. The SC has issued the Guidelines on Digital Assets and Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019, which was recently amended by Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) (Amendment) Order 2025.

Any person intending to issue digital assets or operate a platform that hosts such digital currency or digital token will be subject to the approval and registration requirement of the SC.

However, both the Central Bank of Malaysia (BNM) and the SC have emphasised that, currently, cryptocurrency is not a payment instrument regulated by BNM. Therefore, cryptocurrencies are not considered as legal tender in Malaysia.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

CMA

Cloud computing is regulated in Malaysia primarily by the CMA and the Communications and Multimedia (Licensing) Regulations 2000 (the "Licensing Regulations").

Pursuant to the Information Paper on Regulating Cloud Services published by the Malaysian Communications and Multimedia Commission (MCMC) on 17 December 2021 and updated on 30 September 2024 (the "Information Paper"), the provision of cloud services, defined as "any service made available to end users on demand via the internet from a cloud computing provider's server", is considered as the provision of applications services under the CMA. The provision of applications services is one of the categories of licensable activities under the CMA, alongside the provision of network facilities, network services and content applications services. Unless otherwise exempted from the CMA licensing requirements, the conduct of the foregoing activities requires the facility or service provider to be licensed.

Noting that cloud services could generally be categorised as either software-as-a-service, platform-as-a-service and infrastructure-as-a-service, the Information Paper clarifies that providers of software and solutions which rely on other cloud services platform and infrastructure, known as "pure software providers", are not subject to the foregoing cloud service licensing requirement.

The licensing framework under the CMA imposes the requirement of local presence in the provisioning of the licensable activities. As such, the regulation on cloud services will be based on this premise, whereby a person with local presence would be required to be registered as an ASP class licensee. Pursuant to Ministerial Direction No 2 of 2024 issued on 24 July 2024, CMA class licensees providing cloud services are required to take part in the contribution of universal service provision fund, in accordance with the provision under the Communications and Multimedia (Universal Service Provision) Regulations 2002, for the return of net revenue for the calendar year 2025 onwards.

PDPA

To the extent personal data is processed in the context of cloud and edge computing, the requirements of the PDPA shall be fulfilled.

The obligations under the PDPA are generally imposed on data users (to be known as "data controllers" from 1 April 2025). From 1 April 2025, data processors will also assume certain obligations under the PDPA. This means that, in the context of cloud and edge computing, both the users of cloud and edge computing and the providers may directly be subject to the PDPA, depending on the roles they assume.

The principles and other requirements enumerated in the PDPA must therefore be meticulously assessed within the framework of cloud and edge computing. This includes examining their interplay with the unique characteristics and challenges of these technologies, such as

data transfer, storage and processing across distributed networks. Particular attention must be given to the requirements to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction, and to not keep personal data longer than is necessary.

The Security Standard for personal data processed electronically, as contained in the Personal Data Protection Standard 2015 (PDPS), is of especial relevance to cloud computing:

- the transfer of data through cloud computing services requires the written consent of an officer authorised by the top management of the data user organisation;
- any transfer of data through cloud computing services must be recorded; and
- the transfer of data through cloud computing services must comply with the personal data protection principles in Malaysia and the personal data protection laws of other countries.

According to the Public Consultation Paper No 04/2024 (Personal Data Protection Standards), in an effort to bring the PDPS in line with international best practices, a revised set of standards is being developed by the Personal Data Protection Commissioner. In light of the PDP Amendment Act, both providers and users of cloud and edge computing shall monitor the implementation of the PDPA amendments, and the regulations, standards and guidelines that may be introduced, to ensure ongoing compliance.

Other Data Sharing Laws

It is crucial that other laws and regulations are also considered, such as the Strategic Trade Act 2010 pursuant to which information and data have the potential of being considered as strategic technology controlled by the legislation.

The use by public sector agencies of cloud and edge computing solutions may also have to take into account the upcoming requirements under the Data Sharing Act 2025, which aims to regulate data sharing between public sector agencies, once it comes into force.

CSA

As the "information, communication and digital" sector is among the NCII sectors under the CSA, providers of cloud and edge computing may potentially be designated as NCII Entities which will be subject to the CSA obligations applicable to NCII Entities.

On the other hand, entities designated as NICC Entities (whether from the information, communication and digital sector or any of the ten other listed sectors) that adopt cloud and edge computing shall also ensure that their use of cloud and edge computing is in a manner compatible with the requirements of the CSA, including any code of practice issued thereunder.

Sectoral Requirements

The provision and use of cloud and edge computing shall also have regard to sector-specific laws. For example, the use of technology including the use of cloud and edge computing by financial institutions is subject to stricter requirements imposed by BNM mainly through various policy documents, including the following.

Policy Document on Risk Management in Technology

The Policy Document on Risk Management in Technology, issued 1 June 2023 (RMiT PD), requires risk assessment to be conducted prior to cloud adoption (including risks associated with migration of existing systems, location of cloud infrastructure, exposure to cyber-attacks, termination of cloud service providers), consulta-

tions with BNM prior to public cloud adoption for critical systems (including demonstrating readiness to adopt public cloud for critical systems, and measures mitigate identified risks based on Appendix 10 of the RMiT PD), notifying BNM on the subsequent adoption of public cloud for critical systems (including providing assurance on enhanced incident response due to adverse events), and inclusion of a roadmap for cloud adoption (for both critical and non-critical systems) in the annual outsourcing plan submitted to BNM.

The RMiT PD also prescribes requirements on the management of third-party service providers, defined to include cloud computing software, platform and infrastructure service providers, and would presumably also include providers of edge computing solutions. Among others, service level agreements must be in place when engaging such providers, and must contain the mandatory terms required by the RMiT PD, some of which are specific to the use of cloud services.

Note that revision to the RMiT PD may be underway, in light of the Exposure Draft on Risk Management in Technology released by BNM on 7 November 2024, opened for public feedback until 31 January 2025.

Policy Document on Outsourcing

The Policy Document on Outsourcing, issued 23 October 2019 (the "Outsourcing PD"), requires outsourcing arrangements which qualify as material outsourcing (which would include outsourcing relating to cloud and edge computing that is material) to be approved by BNM in writing before the financial institution enters into such arrangements or makes significant modification to such existing arrangements, and all planned outsourcing arrangements (whether material or otherwise) to be notified to BNM through the submissions of the yearly outsourcing plan.

Specifically for material outsourcing for the use of cloud service providers, in an application for the aforementioned BNM's approval, details of the cloud service, deployment model, nature of data to be held and locations (eg, city and country) where such data is stored, including back-up locations, must be provided. Some of such information is also required to be included in a register of all of the financial institution's outsourcing arrangements.

Due to the oft-cross-border nature of cloud service delivery, the requirements on outsourcing outside Malaysia (ie, where the service provider is located or performs the outsourced activity outside Malaysia), including those relating to the due diligence process and the financial institution's business continuity plan, shall also be carefully considered.

Effective measures to address risks associated with data accessibility, confidentiality, integrity, sovereignty, recoverability and regulatory compliance should be taken, particularly due to the geographically dispersed cloud computing infrastructure.

The Outsourcing PD requires outsourcing arrangements to be governed by written agreements containing the mandatory terms stipulated therein, some of which are specifically related to cloud services, for example to address the right of the financial institution to conduct audits and inspections on the cloud service provider, including reliance on third party certifications and reports made available by cloud service providers, and the testing of a cloud service provider's business continuity plan.

Policy Document on Business Continuity Management

The Policy Document on Business Continuity Management, issued 19 December 2022 (BCM PD), aims to, among others, facilitate the development and implementation of a robust business continuity management framework by financial institutions and strengthen the capacity and preparedness of financial institutions to respond and recover from operational disruptions.

To this end, the BCM PD prescribes policy requirements on matters such as business impact analysis, recovery strategy, crisis management plan, business continuity plan and disaster recovery plan, crisis communication, interdependencies, alternate site and recovery site, and testing. Such requirements are not limited in their application to cloud and edge computing adopted by financial institutions.

However, the interplay between such requirements and the operational and technical aspects of cloud and edge computing must be considered. In the context of cloud services, for example, if a cloud solution is chosen in connection with the requirement to have an alternate and recovery site in the event any infrastructure or systems supporting critical business functions of the financial institution becomes unavailable, the financial institution must consider various issues identified in the BCM PD, including the distance of the cloud infrastructure from the primary site, the use of separate of alternative telecommunications network and power grid from the primary site, and the use of IT systems compatible with the primary site.

Similar to the RMiT PD and Outsourcing PD, the BCM PD requires mandatory contractual terms to be included in outsourcing and contractual arrangements with key service providers, which would include providers of cloud and edge computing if their services support the financial institution's critical business functions.

Policy Document on Management of Customer Information and Permitted Disclosures

The Policy Document on Management of Customer Information and Permitted Disclosures, issued 3 April 2023 (MCI PD), sets out BNM's requirements and expectations regarding financial service providers' measures and controls in handling customer information. Like the BCM PD, the MCI PD does not contain provisions specific to cloud and edge computing, but the provisions therein are nevertheless crucial given their common use for managing, storing and transmitting customer information.

Other BNM policy documents of general application shall also similarly be considered.

Regulated subjects in other sectors may also be subject to sectoral requirements similar to those imposed by BNM on financial institutions. For instance, for the communications and multimedia sector, the Technical Code for Information and Network Security - Cloud Service Providers Selection (First Revision), which was developed pursuant to Section 185 of the CMA, specifies requirements for organisations to select cloud service providers using a risk-based approach that is structured to be generic but tailored for the communications and multimedia industry.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

There is no dedicated legislation on AI in Malaysia as that of the EU's Artificial Intelligence Act.

The development and use of AI is nevertheless subject to compliance with existing laws, including those on consumer protection, data protection and protection of intellectual property rights.

Intellectual Property

As is often the case with AI, computer programs are involved in the creation of products or processes, which has given rise to issues concerning their creation and ownership as regards intellectual property laws, including patent and copyright.

While courts in the past have held that an author under Section 3 of the Copyright Act 1987 may also include a body corporate (eg, the company that developed the AI), the other provisions of the Copyright Act 1987 may not seem to align with this interpretation, for example, the duration of copyright in relation to literary, artistic and musical works extends for a period of 50 years after the death of the author. This inherently suggests that an author in relation to these types of works would need to be a natural person capable of expending a certain level of skill, judgement or effort. Further, the human element here arguably is confined to the input of ideas or concepts (eg, input, descriptions or instructions by the user, which are not protectible by copyright) and not the ultimate expression of the work generated by the AI. For these reasons, it is likely that AI would not qualify as an author of its generated works, nor would the human users whose input may simply be confined to ideas or concepts. By extension therefore, it is arguable that copyright may not subsist in these AI-generated works.

As regards patents, the treatment of AI contributions in the invention process gives rise to conceptual difficulties, particularly due to the Patents Act 1983's definition of an "inventor" which suggests that inventors must be natural persons. This is supported by Section 18, which assigns the right to apply for a patent to the inventor. Moreover, the Patents Regulations 1986 require patent applications to include either the personal identification of inventors or signed written declarations when anonymity is sought. Therefore, it is unlikely in Malaysia for AI inventions to be patentable.

Apart from authorship and inventorship, it is also crucial to ensure that AI-generated works do not infringe the intellectual property rights of third parties, as the use of infringing materials may nevertheless entail liabilities under the relevant intellectual property laws, regardless of the fact that such materials were generated by AI.

Liability

To date, there is no specific legislation to address the liability for personal injury or commercial harm resulting from AI-enabled technologies.

Consumer Protection

From a consumer protection perspective, AI-related products and services may be regarded as consumer products and services that are subject to the consumer protection laws discussed in **1. Digital Economy**.

Data Protection

AI technologies can potentially process a vast amount of personal data, which requires the design and use of AI to comply with the relevant laws on personal data protection discussed in **1. Digital Economy** and **2. Cloud and Edge Computing**. As personal data shall generally not be processed without the consent of the relevant data subjects, this poses a challenge to the use of AI, where certain datasets and information are automatically scrapped from the internet, potentially without the consent and knowledge of the data subjects involved. The PDPA is also

silent on how consent may be obtained and how privacy notice may be given to the relevant data subjects under such circumstances where the data user may not have means to directly communicate with the data subjects involved.

AI-Related Initiatives

The National Guidelines on AI Governance & Ethics (the "AI Guidelines") were launched by the Ministry of Science, Technology and Innovation on 20 September 2024. The AI Guidelines are part of Malaysia's response to the global calls on the ethics of AI, including UNESCO's Recommendation on the Ethics of AI and ASEAN's AI Governance and Ethics Guidelines. Given the dynamic nature of AI, the AI Guidelines may be amended from time to time to reflect technological progress and the changing ethical norms.

The objectives of the AI Guidelines are as follows:

- supporting the implementation of the Malaysian National AI Roadmap 2021-2025;
- facilitating the implementation of responsible AI according to the seven AI Principles;
- building trustworthiness in AI, which is emphasised by responsible AI;
- managing risks caused by the development and deployment of AI technology; and
- maximising the benefits of AI to enhance national productivity, economic growth and competitiveness.

On 12 December 2024, Malaysia launched the National Artificial Intelligence Office, aimed at shaping policies intended to centralise AI policymaking and address regulatory issues. This move positions Malaysia as a key player in AI governance, with the office expected to serve as a focal agency.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There is no dedicated legislation governing Internet of Things (IoT) in Malaysia. That said, the CMA's framework on the governance of communications would apply to the design of IoT and the use thereof.

In particular, the design of IoT and IoT devices must be in accordance with the technical standards imposed by the CMA, to the extent the IoT devices are communications equipment. Under the Communications and Multimedia (Technical Standards) Regulations 2000 (the "Technical Standards Regulations"), it is an offence to intentionally design, install, operate, maintain or modify any communications equipment in a manner which, among others, is contrary to the applicable standards or likely to cause non-interoperability between any communications equipment.

In this regard, several technical codes (which are voluntary industry codes) concerning IoT have been registered under the CMA, including without limitation the Technical Code on Internet of Things (IoT) - Baseline Security Requirements for Consumer Devices, and the Technical Code on Industrial Internet of Things (IIoT) Connectivity And Communication Framework.

Other generally applicable laws on privacy, secrecy and data protection, shall also be considered based on the capabilities and operations of the IoT solution and devices used.

4.2 Compliance and Governance

IoT devices are highly susceptible to cyber-attacks due to their widespread deployment,

limited security features and constant connectivity. In this regard, compliance and governance within an organisation shall focus on the security requirements pursuant to the PDPA, and if used by an NCII Entity, the requirements under the CSA. An organisation's internal governance shall address the use of IoT and the safeguards to be adopted.

It is also crucial that the use by an organisation of IoT devices which qualify as communications equipment have been properly certified and bear the relevant certification mark or label as the Technical Standards Regulations makes it an offence for a person to, among others, use or sell any communications equipment which is contrary to the standards, not certified as required, or does not bear a certification mark or label. Such requirements shall be incorporated into an organisation's internal policies.

4.3 Data Sharing

In terms of data sharing for IoT, the relevant legal considerations are similar to those outlined in **1. Digital Economy** and **2. Cloud and Edge Computing**, although the assessment shall also focus on the pertinent aspects of IoT, eg, the reliance on decentralised edge data processing and what the legal requirements such as the PDPA may mean in such circumstances, including whether such processing is necessary and not excessive.

Given the prevalent use of IoT in the medical and healthcare sector, such use shall also be assessed based on the applicable requirements relating to medical and healthcare data and records. For instance, the PDPA considers information as to the physical or mental health or condition of a data subject to be sensitive personal data, the processing of which generally requires the explicit consent (as opposed to mere consent) of the data subject. Therefore, the use of IoT in the medical and healthcare sector may, for instance, require the explicit consent of the patients for the processing of their medical and healthcare data for the purposes to be achieved by the use of medical IoT devices.

Whether the use of IoT within the medical and healthcare sector is compatible with the medical record keeping and retention requirements, such as those under the Private Healthcare Facilities and Services (Private Hospitals and Other Private Healthcare Facilities) Regulations 2006, shall also be considered.

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Licensing

The provision of audiovisual media services is generally subject to the regulatory framework under the CMA. Generally, a network service provider licence or a CASP licence may be required, depending on the services involved:

- the provision of broadcasting distribution services requires a network service provider individual licence; and
- the provision of satellite broadcasting, subscription broadcasting, terrestrial free to air TV and terrestrial radio broadcasting requires a CASP individual licence.

Other audiovisual media services may also be subject to the CMA licensing requirements (eg, a content applications service of limited appeal or which is targeted to a special interest group and available through subscription by persons using equipment specifically designed for receiving the said service, which requires a CASP class licence), although the provision of internet con-

tent applications services, defined to mean a content applications service which is delivered by means of the internet, is exempted from such licensing requirements.

Therefore, the provision of audiovisual media services online, such as through video streaming platforms, will generally not be subject to the CMA requirement for licence. Note, however, that where such services allow the sharing of user-generated contents, it is nevertheless possible for the provision of such services to require a licence, if such services also fall within the scope of social media services, as discussed under **10. Social Media**.

Content

The regulation of content from the perspective of the CMA and the Content Code has been addressed in **1. Digital Economy**. Specifically for audiovisual media services, the sections within the Content Code on online contents and broadcasting will also be of relevance. For instance, where a service provider allows user-generated content to be shared, but has neither control over the composition of such content nor any knowledge of such content, the Content Code considers such service provider an innocent carrier who is not responsible for the content provided. Nonetheless, this has to also be considered in light of the Federal Court's decision in Peguam Negara Malaysia v Mkini Dotcom Sdn Bhd & Anor [2021] 3 CLJ 603.

Specifically for broadcasting, the Content Code recognises that viewers need adequate information about content to make informed viewing choices based on their personal tastes and standards. The Content Code recommends that broadcasters provide an indication as to the type of content shown by adopting the classifications issued by the Film Censorship Board and any amendments thereto from time to time.

Other areas of law may also regulate contents provided through audiovisual media services. For example, film censorship is regulated by the Film Censorship Act 2002 and prohibits, among others, film or film-publicity material which is obscene or is otherwise against public decency. Audio recordings, or anything which by its form, shape or in any manner is capable of suggesting words or ideas (which presumably include videos), may also be gazetted as prohibited publication under the Printing Presses and Publications Act 1984. The production, distribution and exhibition of films are also subject to the Perbadanan Kemajuan Filem Nasional Malaysia Act 1981, which establishes the National Film Development Corporation Malaysia to spearhead the development of the Malaysian film industry. Separately, seditious contents are prohibited by the Sedition Act 1948.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

The primary legislation governing the telecommunications industry in Malaysia is the CMA. Both the CMA and the Licensing Regulations establish the licensing framework for the sector and regulate areas such as spectrum allocation, consumer protection, content regulation, competition and investigatory powers.

Licensing

As discussed in **2. Cloud and Edge Computing**, there are four categories of licensable activities under the CMA, namely the provision of network facilities, network services, applications services and content applications services.

- Network facilities refer to physical infrastructure used principally for, or in connection with, the provision of network services, excluding customer equipment. Examples of network facilities are fixed links and cables, radio communications transmitters and links, submarine cable landing centres, etc. These represent the fundamental building blocks of the convergence model upon which network, applications and content services are provided. Network services involve the transmission of communications by means of guided and/or unguided electromagnetic radiation, including bandwidth services, broadcasting distribution services, cellular mobile services and switching services. Network services provide the basic connectivity and bandwidth to support a variety of applications.
- Applications services are services provided by means of, but not solely by means of, one or more network services. They include public cellular services, IP telephony, messaging services, internet messaging services and social media services. Applications services are essentially the functions or capabilities which are delivered to end-users. These are retail services.
- Content applications services are applications services which provide content, such as satellite broadcasting, and services such as online publishing (currently exempt from licensing requirements).

Under the CMA, there are two types of licences.

- An individual licence requires a high degree of regulatory control for a specified person to conduct a specified activity and may include special licence conditions. The MCMC also has the power to modify, vary, revoke or impose further special or additional conditions at any time.
- A class licence is a "light-handed" form of regulation designed to promote industry growth and development with easy market access. Unlike an individual licence, a class licence requires merely registration with the MCMC, which is an administrative process.

A provider will have to assess whether its provision of facilities or services falls within any of the categories of licensable activities above, and thereafter determine, based on the Licensing Regulations, if an individual or class licence is required for the specific facilities or services it provides. It may also be the case that its provision of facilities or services is exempted from the licensing requirements by virtue of the Communications and Multimedia (Licensing) (Exemption) Order 2000 (the "Exemption Order"). Examples of exempted activities include the provision of Internet content applications services and web hosting services.

Certification of Communications Equipment

The Technical Standards Regulations provide for certain matters concerning communications equipment, such as the certification of communications equipment, and standards applicable to such equipment. Some aspects of the Technical Standards Regulations have been discussed in **4. Internet of Things**.

"Communications equipment" means any network facilities, customer equipment or radiocommunications equipment, and would include equipment or device using wireless technologies such as laptop or tablet. Regulation 14 of the Technical Standards Regulations states that all communications equipment which is required to be certified under the Regulations shall so be certified. Therefore, to the extent the provision of telecommunications products and services would involve any communications equipment

(including operational infrastructure such as network facilities and consumer devices, eg, smartwatches), such equipment shall properly be certified.

The registered certifying agency under Section 186 of the CMA for purposes of certifying communications equipment is SIRIM QAS International Sdn Bhd.

Security

The MCMC has also released the Guidelines on Information and Network Security for the Communications and Multimedia Industry (INSG, dated 29 October 2024), which provide best practice recommendations to enhance the information and network security and resiliency of the communications and multimedia industry in the country. The INSG serves as a best practices framework and is not mandatory at this point, based on a media statement issued by the MCMC on 8 December 2024.

6.2 Net Neutrality Regulations

To date, Malaysia does not have specific legislation enforcing net neutrality.

6.3 Emerging Technologies

The rapid adoption of 5G, IoT and AI is reshaping Malaysia's telecommunications sector, driving both technological advancements and regulatory considerations. As Malaysia expands its 5G ecosystem, the government has decided to transition from a Single Wholesale Network to a Dual Wholesale Network model. While this shift aims to enhance competition and network resilience, it has raised key concerns particularly regarding network slicing capabilities for private 5G, coverage differentiation, network automation and AI-driven efficiencies and ESG considerations.

These factors are influencing policy decisions, infrastructure development and regulatory approaches within the telecommunications sector. In response to emerging technologies and the rapidly evolving digital landscape, Malaysia has introduced significant legislative changes to address emerging challenges, including the CSA, PDP Amendment Act and OSB as discussed in **1.1 Key Challenges**, as well as other legislative initiatives as discussed in the chapter on Trends and Developments.

7. Challenges with Technology Agreements

7.1 Legal Framework Challenges

One of the main legal challenges encountered by organisations entering into a technology agreement is data protection, given the complexities of data protection requirements. The contractual negotiations may be made more challenging if foreign data protection laws apply, which may mandate the inclusion of model or standard contractual clauses which are not required by the PDPA. The contracting parties should carefully navigate the interaction between the domestic and foreign data protection frameworks. Contention may revolve around contractual clauses on the cross-border transfer of data and the technical and organisational measures to be adopted.

Some other challenges in the contracting process may relate to contractual clauses on intellectual property, liability and risk allocation, eg, indemnification issues.

Contracting parties from certain regulated industries may also face additional layers of challenges when negotiating technology contracts. As discussed in **2. Cloud and Edge Computing**,

financial institutions are subject to more stringent requirements imposed by BNM through various policy documents, including the RMiT PD, Outsourcing PD, BCM PD, and MCI PD (collectively the "BNM Policies"). The BNM Policies typically require financial institutions to include certain mandatory clauses in their contracts with third parties, where the contract or arrangement involves the use of technology, engagement of external service providers and handling of customer information, etc.

Apart from the inclusion of mandatory contractual provisions required by the BNM Policies, financial institutions must also ensure that the other contractual clauses are not inconsistent with other requirements of the BNM Policies (eg, uptime or other service level requirements).

7.2 Service Agreements and Interconnection Agreements

In the context of technology service agreements and telecommunications interconnection agreements, which are typically technical in nature, contracting parties should carefully consider the key definitions. The scope of the services or interconnection arrangement (as the case may be), shall also be clearly defined, including implementation plans, service levels, deliverables, and remedies for service or connection failures. Other essential terms cover fees, termination, responsibilities, security, data protection, intellectual property, exclusion of liability, indemnification and dispute resolution. Clear modification procedures and force majeure clauses ensure adaptability while safeguarding both parties' interests.

While many such provisions may appear commonplace, it is crucial to assess the effect of each provision with reference to the contemplated technology service or interconnection arrangement at hand. For instance, although it is common for technology service agreements to exclude the service provider's liability for loss of data, this may appear unreasonable to a customer in an agreement for the provision of data storage service, since the secure storage of data is essentially what the customer requires in this situation. The parties may therefore have to consider a compromise that is reasonable in the context of data storage, although this does not necessarily mean that there must be no exclusion of liability for loss of data. Such tailored approach should similarly be adopted when negotiating other key provisions.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Electronic signatures are addressed in the following statutes in Malaysia.

- The ECA provides for legal recognition of electronic messages in commercial transactions and the conditions for use of the electronic messages to fulfil the requirements and to enable and facilitate commercial transactions through the use of electronic means and other matters connected therewith. "Commercial transaction" is defined in the ECA to mean a single or multiple communication of a commercial nature, whether contractual or not, which includes any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.
- The Digital Signature Act 1997 (DSA) provides for, and regulates the use of, digital signature as defined in the DSA and to provide for matters connected therewith.

- The Electronic Government Activities Act 2007 (ECGA) provides for legal recognition of electronic messages in dealings between the government of Malaysia and the public, the use of electronic messages to fulfil the requirements and to enable and facilitate commercial transactions through the use of electronic means and other matters connected therewith. The ECGA will apply to federal laws which are designated in accordance with Section 6 therein.

Malaysian law recognises different concepts of "electronic signature" and "digital signature" based on its respective definitions:

- "electronic signature" means any letter, character, number, sound or any other symbol or any combination thereof created in an electronic form adopted by a person as a signature;
- "digital signature" means a transformation of a message using an "asymmetric cryptosystem" (as defined in the DSA) such that a person having the initial message and the signer's public key can accurately determine:
  (a) whether the transformation was created using the private key that corresponds to the signer's public key; and
  (b) whether the message has been altered since the transformation was made.

The ECA recognises the use of an electronic signature where the conditions prescribed therein are met. The ECA does not apply to the following transactions or documents:

- power of attorney;
- the creation of wills and codicils;
- the creation of trusts; and
- negotiable instruments.

Where an electronic signature is a digital signature as defined in the DSA, the provisions of the DSA must be complied with for that digital signature to be effective. The Digital Signature Regulations 1998 sets out a mandatory licensing scheme for certification authority (being the issuers of digital certificates), recognised repositories and recognised date/time stamp authority in respect of digital signatures. Certification authorities licensed under the DSA issue certificates which are computer-based records which:

- identify the certification authority issuing it;
- name or identify its subscriber;
- contain the subscriber's public key; and
- are digitally signed by the certification authority.

9. Gaming Industry

9.1 Regulations

There are several pieces of legislation that regulate gaming in Malaysia, the purpose of which being more to regulate gambling activities in Malaysia. While some forms of gambling are permitted (eg, licensed lottery under the Lotteries Act 1952), gambling activities (including those taking place online) are generally prohibited.

Common Gaming Houses Act

The Common Gaming Houses Act 1953 (CGHA) sets out offences relating to, among others, common gaming houses, gaming machines and public lottery. Under Section 2(1) of the CGHA, gaming is defined as the "playing of any game of chance or of mixed chance and skill for money or money's worth and includes the playing of any game specified in Column 1 of the First and Second Schedules and the playing or operation of any gaming machine". A "gaming machine" is defined to mean "any mechanical, electrical

or electronic machine or device (including any computer program used in such machine or device), whether wholly or partly mechanically, electrically or electronically operated, that is so designed or that has been so adapted that:

- it may be used for the purpose of playing a game of chance or a game of mixed chance and skill; and
- as a result of the playing or operation of the machine or device, winnings in money or money's worth may become payable".

Section 4B of the CGHA prohibits the dealing in gaming machines, including among others the importation, manufacture, assembly, supply, sale, lease and repair of gaming machines or part thereof. Dealing in gaming machines in contravention of Section 4B is an offence punishable by fine and imprisonment.

One of the key challenges with the CGHA is that it does not have any specific provisions on online gambling. This was because the CGHA was enacted before the rise of digital technology and amendments relating to online gambling have yet to be made.

CMA

As for gaming in general (whether involving gambling or otherwise), the discussions on content regulations in **1. Digital Economy** and **5. Audio-visual Media Services** would similarly apply.

The CMA considers "content" to mean any sound, text, still picture, moving picture or other audio-visual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved or communicated electronically. As such, contents within the gaming industry would potentially fall within the purview of the CMA.

Section 233 of the CMA prohibits the use of any network facilities, network service or applications service to knowingly make, create or solicit, and initiate the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person. Section 211 of the CMA also provides that no CASP, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.

Further, the Content Code which has been discussed above is expressly applicable to all CASPs, which may potentially include providers of gaming contents depending on context. Under the Content Code, the material disseminated must not include anything which offends good taste or decency, is offensive to public feeling, is likely to encourage crime or lead to disorder, or is abusive or threatening in nature. The standards by which content is measured, given the requirements, will be viewed in the context of the country's social, religious, political and educational attitudes and observances as well as the need to accommodate global diversity in a borderless world. Part 2 of the Content Code elaborates on the various types of content which is either prohibited or restricted, such as indecent, obscene, violent, menacing, offensive and false content.

Such prohibitions and restrictions must be carefully considered in the development of online games. For example, in relation to indecent content, the Content Code provides that the depiction of nudity is not allowed other than exceptions for non-sexual content nudity based on art, information and/or sciences, and even

then such depictions shall not be excessive or explicit in nature (ie, not too prolonged, close up or gratuitous). Whereas, in relation to violence, the Content Code provides that it shall be portrayed responsibly and not exploitatively.

While Malaysia has no content rating or classification system specifically for digital games, reference could be made to the discussions on content classification in **5. Audiovisual Media Services**, albeit in the context of broadcasting.

9.2 Regulatory Bodies

There is no regulatory body tasked specifically to oversee the gaming industry in Malaysia.

Communications and multimedia activities are under the purview of the MCMC. The Content Code is enforced by the Content Forum.

The enforcement of the CGHA is under the jurisdiction of the Royal Malaysia Police. Criminal prosecutions against online gambling have been instituted under the CGHA, although it does not have any specific provisions on online gambling.

The Federal Court in Lei Meng v Inspektor Wayandiana Abdullah & Ors And Other Appeals [2022] 3 CLJ 177; [2022] MLJU 141 held that whilst the term "online gambling" was not specifically defined in the legal dictionaries, it "envisages a gambling service accessed remotely, ie, online, through the internet where the participants gamble by depositing funds and playing games of chance, like sports betting, online poker, etc." In the case of PP v Multi Electrical Supply & Services & Ors [2022] 5 CLJ 113, the High Court observed that it was quite obvious that, despite the government's ongoing war against illegal gambling, both the CGHA and the Betting Act 1953 have not caught up with the times and they have not been updated to include express provisions for making online gambling illegal. Notwithstanding the position taken in these cases, the Court of Appeal ruled in October 2023 that online gambling was an offence under the CGHA.

9.3 Intellectual Property

Some of the key IP challenges faced by game developers in Malaysia will be that relating to copyright infringement stemming from unauthorised copying and distribution of games. User-generated content (UGC) also poses a challenge with regards to issues of ownership in IP rights. Other challenges will be those relating to the sale of unauthorised digital goods, which broadly include selling game accounts, in-game assets or currency, or offering account "boosting" services to users.

UGC platforms should have a clear notice and take-down policy implemented to ensure that potentially infringing UGC can be reported by platform users and that rights holders can request the withdrawal of specific content with ease. Further, UGC platform operators should have a filtering system to remove offensive or defamatory content because there is a presumption that the platform or portal provider must assume responsibility for taking the risk of facilitating a platform.

A person whose name, photograph or pseudonym appears on any publication depicting themself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or re-publish the publication is presumed to have published or re-published the content of the publication unless the contrary is proved, pursuant to Section 114A of the Evidence Act 1950. Creators can rely on copyright to protect the artistic elements of games, such as drawings of the characters. Trade marks on the other hand

can be relied on to protect distinctive logos, game titles and branding elements.

Lastly, patents protection may be relied on to safeguard technological innovations, including game mechanics, software algorithms and virtual reality features.

10. Social Media

10.1 Laws and Regulations for Social Media

There is currently no specific Malaysian legislative framework governing social media.

CMA

As noted from **6. Telecommunications**, the provision of social media services is a licensable activity under the CMA, because it is considered as the provision of applications services which requires the provider to be registered as an ASP class licensee. The same applies to the provision of internet messaging services, which are often provided alongside social media services. "Social media service" is defined by the Licensing Regulations to mean an applications service which utilises internet access service that enables two or more users to create, upload, share, disseminate or modify content; whereas, "internet messaging service" refers to an applications service which utilises internet access service that enables a user to communicate any form of messages with another user.

The requirement for providers of social media and internet messaging services to be licensed under the CMA came into effect on 1 January 2025. Notwithstanding the foregoing, pursuant to the Exemption Order, a provider who has less than eight million users in Malaysia is exempted from that requirement.

Following a public consultation and the eventual release of the Public Consultation Report on the draft Code of Conduct (Best Practice) for Internet Messaging Service Providers and Social Media Service Providers on 18 December 2024, the MCMC has on 20 December 2024 published the Code of Conduct (Best Practice) for Internet Messaging Service Providers and Social Media Service Providers, which sets out the best practice for adoption by internet messaging service providers and social media service providers licensed under the CMA in addressing harmful content online, as well as other relevant conduct requirements. The Code of Conduct aims to ensure that service providers uphold online safety and security, particularly for children and vulnerable groups. This introduction precedes the coming into force of the OSB discussed below.

OSB

The OSB was recently passed to govern, among others, any applications service which utilises internet access service that enables communications between users. As noted above, social media services are a type of applications service, and hence within the purview of the OSB.

The proposed legislation assigns duties to ASPs licensed under the CMA (which include social media service providers), some of which are as follows:

- duty to implement measures to mitigate risk of exposure to harmful content;
- duty to enable the user to manage online safety;
- duty to protect online safety of child user;
- duty to establish a mechanism for making priority harmful content inaccessible; and
- duty to prepare an online safety plan.

10.2 Regulatory and Compliance Issues

The MCMC is entrusted with administering the OSB, pursuant to which the MCMC's powers include:

- issuing directions in writing to any licensed ASPs, CASPs and network service providers regarding their compliance with the provisions of the OSB;
- directing a person to give any information, particulars or document that is relevant to the MCMC if the MCMC has reasonable grounds to believe that such information, particulars or document is relevant to the performance of the MCMC's functions;
- taking and retaining for as long as is necessary, possession of a document produced or given under the OSB; and
- issuing notices of non-compliance and/or a financial penalty to licensed ASPs, CASPs and network service providers where the MCMC has reasonable grounds to believe that the licensed providers have failed to comply with any of their duties.

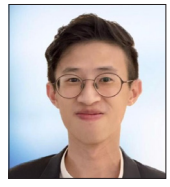
Trends and Developments

Contributed by:
Janet Toh, Boo Cheng Xuan and Yee Yong Xuan
Shearn Delamore & Co.

Shearn Delamore & Co. was established in 1905, and is one of the leading and largest law firms in Malaysia. With over 120 lawyers and 230 staff, the firm has the resources to run and manage the most complex projects, transactions and matters. The firm maintains extensive global network links with foreign law firms and multilateral agencies, and is a founding member of the blue-chip legal network Drew Network Asia (DNA). The firm's technology, multimedia and telecommunications practice group, comprising lawyers from various disciplines including IP, financial services, corporate and M&A, tax and competition, assists clients with the legal issues emerging from the convergence of technology, media and communications. It provides clients with comprehensive and practical legal solutions tailored for an increasingly digital world. The approach and solutions are tailored to meet clients' specific strategic and commercial objectives.

Authors

Janet Toh has over 20 years of experience in intellectual property and technology law. She co-heads the technology, multimedia and telecommunications practice group and leads the personal data protection practice group at Shearn Delamore & Co. Janet advises on IP protection, advertising, e-commerce, franchising, gaming, regulatory approvals and telecommunications. She handles technology and commercial transactions, including outsourcing, software licensing, and IT system development across industries. Janet also counsels clients on data protection, privacy and cybersecurity. She is the deputy chairperson of the Bar Council Cyber and Privacy Law Committee and a member of ITechLaw.



Boo Cheng Xuan is part of the technology, multimedia and telecommunications practice group at Shearn Delamore & Co. He focuses on advisory and transactional matters related to digital technology and cybersecurity, including digital banking, fintech, the metaverse, AI, data centres, cloud computing, telecommunications, software, e-commerce and gaming. He also assists clients in responding to cyber-attacks and data breaches. Cheng Xuan is a member of the Malaysian Bar's National Young Lawyers and Pupils Committee, LAWSIA's Communications, Technology and Data Protection Committee, and LAWASIA's Emerging Lawyers Committee. He has spoken on and moderated discussions about legal technology at the Taiwan-Malaysia Young Lawyers Forum 2023 and the Malaysia-Singapore Young Lawyers' Summit 2024.

Contributed by: Janet Toh, Boo Cheng Xuan and Yee Yong Xuan, **Shearn Delamore & Co.**

Yee Yong Xuan is an associate in the intellectual property practice group of Shearn Delamore & Co. Yong Xuan graduated from the University of Malaya with an LLB (Hons). She was later admitted to the Malaysian Bar as an advocate and solicitor in 2024. Yong Xuan advises clients on intellectual property protection, with a focus on trade mark prosecution and franchising. As a member of the technology, media and telecommunications practice group, Yong Xuan also advises on matters relating to technology and commercial transactions, encompassing areas such as personal data protection, telecommunications and e-commerce.

Shearn Delamore & Co.

7th Floor, Wisma Hamzah-Kwong Hing
No 1 Leboh Ampang
50100 Kuala Lumpur
Malaysia

Tel: +60 3 2027 2727
Fax: +60 3 2078 5625
Email: info@shearndelamore.com
Web: www.shearndelamore.com

TMT in Malaysia

The last year marked a transformative chapter for Malaysia, as significant legal developments reshaped the technology, media and telecommunications (TMT) landscape. These changes underscore the nation's progress in adapting to the rapidly evolving digital era and addressing the complex regulatory challenges of modern technology.

Among the key legislative introductions were the Cyber Security Act 2024, the Online Safety Bill 2024, the Data Sharing Act 2025, and the Malaysian Media Council Bill 2024. Amendments were also proposed to existing laws such as the Personal Data Protection Act 2010, the Communications and Multimedia Act 1998, the Malaysian Communications and Multimedia Commission Act 1998, and the Penal Code. Additionally, updates to the Communications and Multimedia (Licensing) Regulations 2000 introduced licensing requirements for social media and internet messaging service providers.

To further enhance digital governance, Malaysia launched the National Guidelines on AI Governance & Ethics, encouraging responsible use of AI.

On 12 December 2024, Malaysia launched the National Artificial Intelligence Office. This Office is set to play a pivotal role in shaping AI-related policies, centralising AI governance and addressing regulatory issues. This move positions Malaysia as a key player in AI governance, with the Office expected to serve as a focal agency.

While these legal developments have profound implications for the ICT sector, their impact extends across industries, reinforced by laws such as the Cyber Security Act 2024 and amendments to the Personal Data Protection Act 2010, both designed to safeguard data and bolster cybersecurity nationwide.

This chapter reviews these pivotal developments, presented in a generally reverse chronological order, highlighting their impact on Malaysia's TMT and ICT legal landscape.

Introduction of Malaysian Media Council Bill 2024

The Malaysian Media Council Bill 2024, which aims to establish the Malaysian Media Council, was tabled for its first reading at the Dewan Rakyat on 12 December 2024 and was subsequently passed on 26 February 2025. The proposed legislation seeks to empower the Malaysian Media Council to set standards and establish a code of conduct for media practitioners and independent media practitioners in accordance with the standards of ethical and responsible journalism. The Malaysian Media Council Bill 2024 will next be tabled for reading at the Dewan Negara.

Introduction of the Data Sharing Act 2025

Passed by parliament in December 2024 and published in the Federal Gazette on 20 February 2025, the Data Sharing Act 2025 represents a significant milestone in fostering collaboration and improving data governance within the public sector. By facilitating data sharing between federal government agencies, the Data Sharing Act 2025 aims to enhance the efficiency and transparency of public service delivery. The Data Sharing Act 2025 focuses on enabling the sharing of data controlled by one public sector agency with another.

A "public sector agency" is defined as (i) the government agency in charge of the public services under Article 132(1) of the Federal Constitution, excluding joint public services and State pub-

lic services, and (ii) statutory authorities vested with powers by federal law. The Data Sharing Act 2025 provides, among other things, for the following:

- Sharing of data under the control of a public sector agency with other public sector agency: public sector agencies may request another public sector agency for the sharing of data under the control of such other public sector agency by specifying the data requested, the purpose for which the data is requested, the public service agencies intended to be the data recipient and the data provider, and the manner in which the data will be handled.
- Establishment and membership of the National Data Sharing Committee: a "National Data Sharing Committee", which is responsible to the Cabinet, shall be established. The National Data Sharing Committee's responsibilities include formulating policies and strategies related to data sharing, overseeing the effective implementation of the proposed legislation and taking or recommending appropriate steps and administrative actions to resolve difficulties or administrative issues that may arise during the implementation of the proposed legislation.
- Duties and powers of the Director General of the National Digital Department: the Director General of the National Digital Department is responsible for, among others, implementing the policies and strategies relating to data sharing formulated by the National Data Sharing Committee, and co-ordinating and facilitating data sharing under the proposed legislation.

The Data Sharing Act 2025 will take effect on a date specified by the Minister of Digital.

Amendments to the Communications and Multimedia Act 1998 and Malaysian Communications and Multimedia Commission Act 1998

Passed by parliament in December 2024, the Communications and Multimedia (Amendment) Act 2025 came into force on 11 February 2025, except Sections 92 and 112 thereunder. It brings about pivotal changes to the Communications and Multimedia Act 1998 (CMA), focusing on enhancing regulatory oversight, broadening enforcement powers and introducing stricter penalties. Highlights of the amendments to the CMA include the following.

- Simplified class licence registration: a new Section 46A enables the Minister to dispense with the formalities of registration under a class licence through a Section 13 declaration.
- Broadening of the powers of the Malaysian Communications and Multimedia Commission (MCMC): under the amended Sections 51, 55 and 104, the MCMC is vested with expanded authority to issue directions regarding compliance with the CMA, establish determinations to promote industry conduct that aligns with the objectives of the CMA, and determine mandatory standards, including for matters where the MCMC is satisfied that the designated industry forum has not developed a satisfactory voluntary industry code or that the voluntary industry code is likely to fail or has failed, and will continue to fail.
- Widening of the MCMC's powers to gather information and to conduct audits: the new Section 73A grants the MCMC the authority to conduct audits on licensees whilst the new Section 73B empowers the MCMC to mandate that licensees appoint independent experts for audits at their own expense.

The new Section 252A introduces obligations for preserving communications data where a police officer or an authorised officer is satisfied that (i) the communications data is reasonably required for an investigation, and (ii) there is a risk that the communications data may be destroyed or rendered inaccessible. The new Section 252B on the other hand allows a police officer or an authorised officer to issue a written notice requiring the person in control of the communications system to disclose the required communications data where it is deemed reasonably necessary for investigating offences under the CMA or its subsidiary legislation.

- Network security measures: the new Section 230A allows the MCMC to register certifying agencies for certifying compliance with regulations or standards in relation to network security. The new Section 230B grants the MCMC authority to instruct any person to take the necessary measures to prevent, detect or counter any network security risk.
- Changes to access agreement registration requirements: the existing registration requirements under Sections 90 to 93 will be replaced by a lodgement system for access agreements under the amended Section 150. This amendment shifts the responsibility to the parties of the access agreement to ensure compliance with the CMA.
- Restrictions on harmful content and spam: the amendments aim to strengthen regulations concerning harmful content and spam. In Sections 211 and 233, the term "offensive" is replaced with "grossly offensive." Explanations have been added to Section 233 to provide clearer guidelines on the types of content that are prohibited. Section 233 now explicitly covers actions involving fraud or dishonesty against any person. The new Section 233A prohibits the sending of unsolicited commercial electronic messages.
- Suspension of content applications service: a new Section 211A empowers the MCMC to suspend services provided by a content applications service provider for non-compliance with Chapter 2 of Part IX of the CMA or for breaching conditions of its individual or class licence relating to content.
- Private action for network and fraud damages: Section 236A introduces a right of private action for damage caused to network facilities or fraud involving access devices.
- Increased penalties: penalties for various offences, including non-compliance with mandatory standards (Section 105), improper network use (Section 233) and unlicensed operations (Sections 126 and 206), have been increased.

Separately, the Malaysian Communications and Multimedia Commission (Amendment) Bill 2024, which was tabled for its first reading on 2 December 2024, remains pending further development.

Introduction of Online Safety Bill 2024

The Online Safety Bill 2024 marks a significant step in Malaysia's journey toward a safer online environment. Passed by the Dewan Rakyat on 11 December 2024, and subsequently by the Dewan Negara on 16 December 2024, this proposed legislation is designed to regulate harmful content and establish clear duties for applications service providers (ASPs), content applications service providers (CASPs) and network service providers. The Online Safety Bill 2024 governs:

- any applications service which utilises internet access service that enables communication between users;

- any content applications service which utilises internet access service to provide content; and
- any network service.

However, private messaging features of any applications service and content applications service are explicitly excluded from its scope. Importantly, the proposed legislation applies both within and outside Malaysia, as outlined in Section 3.

At the core of the Online Safety Bill 2024 is its emphasis on addressing "harmful content", which is categorised into the following:

- content on child sexual abuse material as provided for under Section 4 of the Sexual Offences Against Children Act 2017;
- content on financial fraud;
- obscene content including content that may give rise to a feeling of disgust due to lewd portrayal which may offend a person's decency and modesty;
- indecent content including content which is profane in nature, improper and against generally accepted behaviour or culture;
- content that may cause harassment, distress, fear or alarm by way of threatening, abusive or insulting words or communication or act;
- content that may incite violence or terrorism;
- content that may induce a child to cause harm to themself;
- content that may promote feelings of ill-will or hostility amongst the public at large or may disturb public tranquillity; and
- content that promotes the use or sale of dangerous drugs.

The Online Safety Bill 2024 also introduces stricter regulations for "priority harmful content", which includes content involving child sexual abuse material and content related to financial fraud.

The Malaysian Communications and Multimedia Commission (MCMC) is entrusted with administering the Online Safety Bill 2024. The Online Safety Bill 2024 also establishes the Online Safety Committee to advise and give recommendations to the MCMC on matters relating to online safety and the Online Safety Appeal Tribunal to review any written instructions, determinations and directions issued by the MCMC. Further, the proposed legislation assigns duties to licensed ASPs and licensed CASPs, and provides for the reporting of harmful content, some of which are set out below.

- Duty to implement measures to mitigate risk of exposure to harmful content: ASPs and CASPs must implement measures specified in the Code issued by the MCMC under the proposed Section 80 ("Code") to mitigate the risk of users (ie, users of their services) being exposed to harmful content. They may implement alternative measures, subject to the MCMC's approval, if proven to be more effective.
- Duty to issue guidelines to users: ASPs and CASPs must issue clear, accessible and regularly updated guidelines describing the safety measures implemented and terms of use, ensuring they are available to users.
- Duty to enable users to manage online safety: ASPs and CASPs are required to make available tools and settings that allow users to manage their safety online, such as preventing unwanted communication and restricting identification.
- Duty to make available a mechanism for reporting harmful content: ASPs and CASPs must establish a mechanism to enable users

to report harmful content available on their services.
- Duty to make available a mechanism for user assistance: ASPs and CASPs must make available user assistance that is accessible and responsive for users to raise safety concerns, obtain information and make inquiries.
- Duty to protect online safety of child users: ASPs and CASPs must implement measures specified in the Code to ensure safe use of their services by child users, including blocking suspected harmful content from child users, limiting adult-child communication, and regulating personalised content recommendations.
- Duty to establish a mechanism for making priority harmful content inaccessible: ASPs and CASPs must establish a mechanism to make priority harmful content inaccessible to all users.
- Duty to prepare an Online Safety Plan: ASPs and CASPs must prepare an Online Safety Plan addressing their compliance with the prescribed duties, ensure it is accessible and regularly updated, and submit a copy to the MCMC.
- Reporting harmful content: users of the services of ASPs or CASPs may report harmful or priority harmful content to ASPs or CASPs, and/or the MCMC. The ASP or CASP (as the case may be) must assess, respond and take appropriate actions, including dismissing frivolous reports or making content inaccessible.
- Action by ASPs and CASPs on their own motion: ASPs and CASPs may also act independently to restrict harmful content if deemed necessary.
- Enforcement and MCMC oversight: the MCMC may instruct ASPs and CASPs to make content permanently inaccessible. Non-compliance by the ASP or CASP (as the case may be) with the written instruction issued by the MCMC is in this regard an offence punishable by fine.

The Online Safety Bill 2024 will now be presented for Royal Assent, and once gazetted, it will take effect on a date specified by the Minister of Communications.

Amendments to the Penal Code

A significant step toward addressing bullying in all its forms was taken with the passing of the Penal Code (Amendment) (No 2) Bill 2024. Passed by the Dewan Rakyat on 10 December 2024, and subsequently by the Dewan Negara on 16 December 2024, the amendments seek to modernise the Penal Code to address bullying comprehensively, including online bullying. The proposed changes introduce specific provisions to combat bullying in any form.

The new bully-related offences include using or making any threatening, abusive or insulting words or communication, or engaging in any threatening, abusive or insulting act, and such words, communication or act are heard, seen or otherwise perceived by a person who is likely to feel harassed, distressed, fear or alarmed by such words, communication or act. The Penal Code (Amendment) (No 2) Bill 2024 also makes it an offence to circulate or make available any identity information (ie, any information that identifies or purports to identify a person) with intent to cause harassment, distress, fear or alarm to the victim.

The Penal Code (Amendment) (No 2) Bill 2024 will now be presented for Royal Assent. Once gazetted, the amendments will come into effect on a date determined by the Minister.

Amendments to the Personal Data Protection Act 2010

The Personal Data Protection (Amendment) Act 2024 (the "PDP Amendment Act"), which amends the Personal Data Protection Act 2010 (PDPA), is being implemented in three stages:

- 1 January 2025: Sections 7, 11, 13 and 14 of the PDP Amendment Act will take effect;
- 1 April 2025: Sections 2, 3, 4, 5, 8, 10 and 12 of the PDP Amendment Act will take effect; and
- 1 June 2025: Sections 6 and 9 of the PDP Amendment Act will take effect.

Selected legislative amendments brought about by the PDP Amendment Act are summarised as follows.

- The term "data user" will be replaced with "data controller", aligning with global data protection terminology. However, the existing definition for "data user" remains unchanged.
- The penalties for non-compliance with any of the Personal Data Protection Principles will be significantly increased, with fines raised from MYR300,000 to MYR1,000,000 and/or imprisonment extended from a maximum term of two years to a maximum term of three years.
- Previously applicable only to data controllers, the Security Principle will directly bind data processors.
- Data controllers must notify the Personal Data Protection Commissioner ("Commissioner") of any personal data breaches as soon as practicable. Failure to do so could result in a fine of up to MYR250,000 and/or imprisonment for up to two years. The relevant data subject must also be notified where the personal data breach causes or is likely to cause any significant harm to the data subject.
- Both data controllers and data processors must appoint data protection officer(s), who shall be accountable to the data controller or data processor.
- Rights to data portability will be introduced in favour of the data subjects, subject to technical feasibility and compatibility of the data format.
- In terms of cross-border transfer of personal data, the pre-existing "whitelist" approach will be abolished. Data controllers will be able to transfer personal data out of Malaysia so long as the prescribed conditions are met.

The Department of Personal Data Protection has since circulated a series of public consultation papers which generally relate to the issues sought to be addressed by the PDP Amendment Act:

- Public Consultation Paper No 01/2024: The Implementation of Data Breach Notification;
- Public Consultation Paper No 02/2024: The Appointment of Data Protection Officer;
- Public Consultation Paper No 03/2024: The Right to Data Portability;
- Public Consultation Paper No 04/2024: Personal Data Protection Standards; and
- Public Consultation Paper No 05/2024: Cross Border Personal Data Transfer Guidelines.

On 18 November 2024, the Commissioner and Futurise Sdn Bhd issued a joint press release providing updates on Malaysia's Personal Data Protection and Privacy Regulatory Sandbox. As part of the Sandbox's deliverables, four guidelines and one standard will be released by early 2025, while further further guidelines will be released in the third quarter of 2025. These guidelines are set to provide clear, actionable frameworks for the private sectors to ensure

compliance with evolving data protection regulations and international standards.

Introduction of Cyber Security Act 2024

As discussed in the chapter on Law and Practice, the Cyber Security Act 2024 (CSA) came into force on 26 August 2024. Key provisions of the CSA applicable to national critical information infrastructure entities and cybersecurity service providers include the implementation of the measures, standards and processes specified in the code of practice, notification of cybersecurity incidents, the conduct of cybersecurity risk assessments and audits, the licensing of cybersecurity service providers.

Four pieces of subsidiary regulations have been introduced under the Cyber Security Act 2024, namely:

- Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024;
- Cyber Security (Notification of Cyber Security Incident) Regulations 2024;
- Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024; and
- Cyber Security (Compounding of Offences) Regulations 2024.

The Cyber Security (Exemption) Order 2025 has also been issued to exempt entities listed therein from all of the provisions of the CSA.

The Chief Executive of the National Cyber Security Agency has also issued the following directives pursuant to his statutory powers under Section 13 of the CSA:

- Directive No 1: Notification of Cyber Security Incident;
- Directive No 2: Licensing of Cyber Security Service Provider;
- Directive No 3: Designation of National Critical Information Infrastructure Entity;
- Directive No 4: National Cyber Security Baseline Self-Assessment;
- Directive No 5: Cyber Security Risk Assessment; and
- Directive No 6: Extension of Grace Period for Obtaining Cyber Security Service Provider's Licence.

The National Cyber Security Baseline, which is a set of minimum security controls and best practices to ensure a basic level of cybersecurity protection, has also been introduced on the website of the National Cyber Security Agency, alongside a National Cyber Security Baseline Self-Assessment Tool.

Amendments to Communications and Multimedia (Licensing) Regulations 2000 and Communications and Multimedia (Licensing) (Exemption) Order 2000

Pursuant to the Communications and Multimedia (Licensing) (Amendment) (No 2) Regulations 2024 and Communications and Multimedia (Licensing) (Exemption) (Amendment) Order 2024, starting from 1 January 2025, providers of internet messaging services and social media services with 8 million or more users in Malaysia will be required to obtain an applications service provider class licence under the CMA to offer their services within Malaysia.

Following a public consultation and the eventual release of the Public Consultation Report on the draft Code of Conduct (Best Practice) for Internet Messaging Service Providers and Social Media Service Providers on 18 December 2024, the MCMC on 20 December 2024 published the Code of Conduct (Best Practice) for Internet

Messaging Service Providers and Social Media Service Providers, which sets out the best practice for adoption by internet messaging service providers and social media service providers licensed under the CMA in addressing harmful content online, as well as other relevant conduct requirements. The Code of Conduct aims to ensure that service providers uphold online safety and security, particularly for children and vulnerable groups.

National Guidelines on AI Governance & Ethics

The National Guidelines on AI Governance & Ethics (the "AI Guidelines"), launched by the Ministry of Science, Technology and Innovation on 20 September 2024, provide a comprehensive framework for ensuring the responsible development and use of AI. The AI Guidelines offer guidance to three key stakeholder groups, namely:

- society - users, workers and consumers;
- government agencies and policymakers; and
- industry - including developers and designers.

The AI Guidelines are part of Malaysia's response to the global calls on the ethics of AI, including UNESCO's Recommendation on the Ethics of AI and ASEAN's AI Governance and Ethics Guidelines. Given the dynamic nature of AI, the AI Guidelines may be amended from time to time to reflect technological progress and the changing ethical norms.

The AI Guidelines aim to:

- support the implementation of the Malaysian National AI Roadmap 2021-2025;
- facilitate the implementation of responsible AI according to the 7 AI Principles;
- build trustworthiness in AI, which is emphasised by responsible AI;
- manage risks caused by the development and deployment of AI technology; and
- maximise the benefits of AI to enhance national productivity, economic growth and competitiveness.

Concluding Remarks

The past year's TMT legal advancements reflect Malaysia's proactive approach in addressing the challenges and opportunities of the digital era. These regulatory reforms not only strengthen Malaysia's governance framework but also foster sustainable growth, innovation and trust in the ICT sector and beyond. As stakeholders adapt to this evolving legal and technological landscape, ensuring the effective implementation and continuous refinement of these laws remains paramount.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com