Chambers
Global Practice
Guides

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

TMT
2022

Malaysia: Law & Practice
and
Malaysia: Trends & Developments

Charmayne Ong, Natalie Lim and Jillian Chia
Skrine

practiceguides.chambers.com

MALAYSIA

Law and Practice

Contributed by:
Charmayne Ong, Natalie Lim and Jillian Chia
Skrine see p.22

CONTENTS

1. CLOUD COMPUTING

1.1 Laws and Regulations

There is increasing regulation of cloud services through a wide variety of legislative provisions, technical codes and guidelines, some of which specifically relate to cloud services, while others are wide enough to have a considerable impact on such services. Key laws, codes and guidelines are set out below.

Communications and Multimedia Act 1998 (CMA)

The primary legislation governing the telecommunications industry in Malaysia is the CMA, which is enforced by the telecommunications regulator, the Malaysian Communications and Multimedia Commission (MCMC). Cloud service providers are subject to Malaysia's telecommunications laws, namely the CMA and its subsidiary legislation. Effective from 1 January 2022, cloud service providers with a local presence which provide cloud services in Malaysia must also obtain an Applications Service Provider class licence.

A wide variety of technical codes and guidelines may also apply to cloud service subscribers (CSSs) that seek to entrust certain processes or data to cloud service providers (CSPs), depending on the circumstances such as the Technical Code on Information and Network Security – Cloud Service Provider Selection, which specifies certain requirements relating to the selection of CSPs by CSSs. For instance, when selecting CSPs, a CSS is required to, among other things, conduct a risk assessment and select a CSP according to the minimum selection criteria stipulated, which are based on the risk tolerance of the CSS, the industry standards that the CSP has complied with, and the ability of the CSP to provide relevant certification and a third-party audit report.

Personal Data Protection Act 2010 (PDPA)

The PDPA, as the main federal regulatory framework for personal data protection in Malaysia, contains data protection obligations that must be considered when the use of cloud services involves the processing of personal data. Data users, who are different from data processors, are subject to compliance with the obligations under the PDPA, and are defined as persons who either alone or jointly, or in common with other persons, process any personal data or have control over or authorise the processing of any personal data (see **6. Key Data Protection Principles** for the definition of a "data processor" and further details on the PDPA).

Under the PDPA, a data user is required to ensure, for the purpose of protecting personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction, that data processors (eg, a CSP) that process personal data on their behalf provide sufficient guarantees in respect of the technical and organisational security measures governing the processing of such personal data, and that the data processor takes reasonable steps to ensure compliance with those measures.

Data users are also prohibited from transferring personal data outside Malaysia subject to certain exceptions (see **6. Key Data Protection Principles** for further details on cross-border transfers).

Furthermore, the Personal Data Protection Standard 2015 ("PDP Standard") imposes obligations on data users to ensure that, among other requirements, transfers of personal data through cloud computing services are recorded and that the written consent of an officer authorised by the top management of the data user organisation is obtained before such a transfer is made. Personal data transferred through a

cloud computing service must not only comply with the personal data protection principles in Malaysia but also with personal data protection laws of other countries.

Currently, the PDPA does not contain direct obligations on data processors and does not provide for a general data localisation requirement, although there has been a public consultation paper suggesting that these might be introduced in the future. However, data localisation requirements may apply depending on factors such as the industry, eg, electronic money (e-money) licences may impose this requirement as a licence condition.

Industry-Specific Requirements

Additional requirements may apply depending on the specific industry. For instance, in the financial sector, the Central Bank of Malaysia ("BNM") has issued several mandatory policy documents pertaining to risk management in technology, outsourcing and the management and disclosure of customer information, which contain specific requirements on the use of cloud services:

- the Policy Document on Risk Management in Technology;
- the Policy Document on Outsourcing; and
- the Policy Document on Management of Customer Information and Permitted Disclosures.

Among other stipulations, financial institutions (FIs) are required to consult with the BNM before using a public cloud for critical systems and must notify the BNM prior to the use of cloud services for non-critical systems. In respect of outsourcing arrangements, which includes outsourcing arrangements with CSPs, the Policy Document on Outsourcing requires, among other things, that FIs obtain the BNM's approval before entering into an outsourcing arrangement, and that FIs that use cloud services maintain a register containing additional particulars of the arrangement, namely, the nature of the data held and the locations where it is stored.

The Policy Document on Management of Customer Information and Permitted Disclosures also contains requirements for FIs with regard to measures and controls in handling customer information throughout the information life cycle, covering collection, storage, use, transmission, sharing, disclosure and disposal of customer information. FIs must, among other things, ensure that the service-level agreement between them and the CSP adequately reflects the FI's obligation to safeguard customer information.

2. BLOCKCHAIN

2.1 Legal Considerations

From a Malaysian legal standpoint, blockchain is not regulated under a specific regulatory framework but may be governed by several pieces of legislation depending on the functionalities and use of blockchain technology.

Sector-Specific Regulation – Prescription Order

In the Malaysian capital markets and securities sector, blockchain-based digital assets could qualify as a "digital currency" or "digital token" as defined under the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 ("Prescription Order"), and be deemed as securities under the Malaysian Capital Markets and Services Act 2007 (CMSA). Where this is the case, these digital assets will be subject to the purview of the Securities Commission of Malaysia (SC), and the offering and trade of these digital assets, along with the operation of the platform that hosts these digital assets will be subject to the approval and registration requirements of the SC.

The Guidelines on Digital Assets ("DA Guidelines") issued by the SC in 2020 prescribe, among other requirements, that a digital token offering can only be carried out in Malaysia through an initial exchange offering (IEO) operator registered with the SC, and that issuers of digital tokens must comply with certain requirements before offering digital tokens via a registered IEO operator, eg, eligibility and white paper requirements.

Additionally, the CMSA states that the trading of digital assets in Malaysia can only be conducted through an authorised digital assets exchange (DAX) operator, and the Guidelines on Recognised Markets, issued by the SC, prescribe that only digital assets approved by the SC can be traded.

To date, the SC has only approved five digital assets to be traded on a regulated platform/digital assets exchange in Malaysia, ie, Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Litecoin (LTC) and Bitcoin Cash (BCH). On the other hand, only four recognised market operators have been registered with the SC and are permitted to operate a digital assets exchange in Malaysia, ie, Luno Malaysia Sdn Bhd, MX Global Sdn Bhd, SINEGY Technologies (M) Sdn Bhd, and Tokenize Technology (M) Sdn Bhd.

Although there is a regulatory framework on the issuance and trading of digital tokens and digital currencies, the BNM has publicly confirmed that cryptocurrencies and digital assets are not considered legal tender in Malaysia.

Sector-Specific Regulation – FSA

Where the blockchain-based digital asset qualifies as e-money, the provisions and requirements of the Financial Services Act 2013 (FSA) apply, including the requirement that issuers of e-money obtain the prior approval of the BNM. A digital asset will be regarded as e-money if it represents a payment instrument that stores funds electronically in exchange for funds paid to the issuer and can be used as a means of making payment to any person other than the issuer.

Where an entity carries out any prescribed activity involving digital currencies as set out and defined in the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001, they will also be subject to additional anti-money laundering and anti-terrorism financing obligations, such as customer due diligence, reporting, and retention of records obligations.

Risk and Liability

Existing legal frameworks, such as contract, tort and consumer protection laws, may continue to apply to risk and liability issues relating to blockchain-based technologies.

As an illustration, in the watershed case of Robert Ong Thien Cheng v Luno Pte Ltd & Anor (2019) 1 LNS 2194, the High Court was of the view that Section 73 of the Malaysian Contracts Act 1950 (CA), concerning the liability of a person to whom money is paid or delivered, by mistake or under coercion, extended to cryptocurrencies and that the CA should be construed to reflect the changes in modern technology and commerce. This decision marks an important step in the development of cryptocurrency in Malaysia and how the legal landscape in Malaysia adapts to the issues brought about by blockchain technologies.

Data Protection

Where use of blockchain technology involves the processing of personal data for commercial purposes, the data protection principles enshrined in the PDPA may apply (see **6. Key Data Protection Principles**). However, some of the fundamental characteristics of blockchain technolo-

gies are generally incompatible with certain data protection principles in the PDPA.

Most notably, the immutable nature of entries held on blockchain is incompatible with the retention principle, which states that personal data may not be processed and retained longer than necessary for the fulfilment of the purpose for which it was processed. Determining who the data user or data processor is in a blockchain context is also challenging in a distributed ledger scenario and while the analysis may depend on the type of blockchain, the multiple stakeholders in the blockchain may not fit within the typical description of a data user, data processor or data subject. For instance, in a public or permission-less blockchain, there is no central operator or administrator of the blockchain since it is typically peer to peer. The PDPA's requirement that a data user should pass on its security obligations and enter into a written contract with a data processor may therefore be impractical. Furthermore, nodes do not necessarily behave like data processors.

Another example is the incongruity between the immutability of blockchain and the data subjects' right to rectify personal data that is inaccurate, incomplete, misleading, or not kept up to date.

Where data is transferred across blockchain nodes which are located in multiple jurisdictions, the transfer of such data could also give rise to issues relating to cross-border transfers of data (see **1. Cloud Computing** and **6. Key Data Protection Principles** for further details on cross-border transfers).

3. LEGAL CONSIDERATIONS FOR BIG DATA, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

3.1 Challenges and Solutions

Although there is no specific legislation governing the application of big data, machine learning and artificial intelligence technologies in Malaysia, government agencies and regulatory bodies in Malaysia are working on expanding the existing legislation and formulating a national framework to regulate such technologies.

Applicable Frameworks

A collaborative effort between the Malaysian government and stakeholders resulted in the launch of the National Artificial Intelligence Roadmap which spans from 2021 until 2025. The roadmap outlines numerous initiatives including:

- developing an AI Governance Framework;
- implementing a cybersecurity policy;
- collaborating with industries to develop specific guidelines on privacy, security, and ethics; and
- establishing an AI Code of Ethics.

In addition, the Malaysia Digital Economy Corporation (MDEC), an agency under the Ministry of Communications and Multimedia, has been tasked with spearheading the National Big Data Analytics Framework ("BDA Framework") which seeks to create a national big data analytics ecosystem to make big data analytics a catalyst for further economic growth in all sectors. MDEC is also currently formulating a National AI Framework which may provide clarity to the regulation of AI in Malaysia.

Data Protection

The inherent characteristics of big data analytics, machine learning and AI in collecting and

processing large quantities of data may give rise to issues concerning the consent of data subjects, or rather the lack thereof. Larger data sets are also at risk of serious data breaches which could result in the unauthorised distribution of a huge amount of personal data. Organisations are therefore encouraged to introduce and implement appropriate security measures, such as those set out in the PDPA and applicable standards (see **6. Key Data Protection Principles**).

Other data protection issues surrounding big data analytics, machine learning and AI include issues surrounding personal data being kept longer than necessary for the fulfilment of its original purpose, personal data being disclosed to parties unknown to the data subjects, and the inability of individuals to determine whether their personal data has been collected.

Intellectual Property

There is uncertainty as to whether and how AI-generated works may be protected under the current intellectual property framework in Malaysia.

While the term "inventor" is not defined in Malaysian patent legislation, the wording of the Patents Regulations 1986 ("Patents Regulations") and the Patents Act 1986 ("Patents Act") suggests an interpretation that excludes AI systems. For example, the Patents Regulations provide that an application must contain the name and address of the inventor, and where inventors do not wish to be named, they must sign and submit a declaration in writing to the Registrar stating such.

Whether the Malaysian Copyright Act 1987 ("Copyright Act") is fully equipped to protect AI-produced works is also doubtful due to potential issues surrounding the ownership of copyright, the possible perpetual copyright in AI-produced works, the availability of moral rights to AI authors, and the enforcement of copyright protection afforded to AI-produced works.

4. LEGAL CONSIDERATIONS FOR INTERNET OF THINGS PROJECTS

4.1 Restrictions on a Project's Scope

Presently, there is no statute in Malaysia that specifically relates to or regulates the Internet of Things (IoT). Nevertheless, there are existing sector-specific guidelines which regulate the IoT and additional laws and regulations which are wide enough to apply to IoT projects. The following are the key examples of such laws, regulations and guidelines.

Telecommunications

In carrying out IoT projects, parties have to abide by the CMA's licensing and regulatory framework where applicable, including its requirements relating to use of spectrum. In particular, where the IoT project involves carrying out one of the licensable activities as set out in the CMA and its subsidiary legislation (eg, ownership or provision of network facilities), an appropriate licence will have to be obtained. The licensee will also be required to comply with various obligations under the CMA, including compliance with licence conditions, equity restrictions for certain licence types, etc (see **8. Scope of Telecommunications Regime**).

Where an IoT project involves the use of spectrum, the use must be pursuant to an appropriate assignment by MCMC and must be in accordance with the Spectrum Plan and any applicable Standard Radio System Plans as issued by MCMC. Additionally, communications equipment (including equipment used for the IoT) must receive appropriate product certification from the certifying body appointed by MCMC,

SIRIM QAS International Sdn Bhd ("SIRIM"), which certifies the equipment for, among other things, safety and compliance with determined technical standards, such as the Technical Code on Short Range Devices.

There are also a number of technical codes which are relevant to IoT, including:

- the Technical Code on Internet of Things – Application Security Requirements;
- the Technical Code on Internet of Things – High-Level Functional Architecture;
- the Technical Code on Internet of Things – Security Management; and
- the Technical Code on Short Range Devices – Specifications (Second Revision).

Other technical codes which may be relevant but have yet to be registered are:

- the Technical Code on the Industrial Internet of Things Connectivity and Communication Framework; and
- the Technical Code on the IoT Interoperability Framework.

Data Protection

In so far as an IoT project involves the processing of personal data in Malaysia, the data user(s) must process the personal data in compliance with the PDPA (see **6. Key Data Protection Principles**).

Cybersecurity

Although Malaysia does not currently have all-encompassing cybersecurity legislation, in October 2021, the Malaysian government announced its plan to table a specific law to strengthen cybersecurity in the country. However, before implementing an IoT project, organisations must consider other applicable legislation that is wide enough to have an impact on such projects. This legislation includes the following:

- the Computer Crimes Act 1997 (CCA);
- the Penal Code;
- the Copyright Act;
- the Digital Signature Act 1997 ("Digital Signature Act");
- the Strategic Trade Act 2010; and
- the Official Secrets Act 1972 (Official Secrets Act).

In 2020, CyberSecurity Malaysia, a cybersecurity specialist agency under the purview of MCMC, released the Guidelines for Secure Internet of Things ("IoT Guidelines") which detail security requirements/controls for manufacturers, providers and consumers to implement in order to achieve a secure IoT system. Although non-binding, the IoT Guidelines aim to assist relevant stakeholders by providing an IoT security framework and setting out existing IoT threats and vulnerabilities for them to be mindful of.

5. CHALLENGES WITH IT SERVICE AGREEMENTS

5.1 Legal Framework Features

Generally, IT service agreements should contain key provisions such as the obligations of the parties, liability, indemnity, representations and warranties, confidentiality obligations as well as termination and post-termination obligations. The following are some of the main challenges and areas of risk in respect of contracting with local organisations.

Data Security

One of the challenges that organisations entering into IT service agreements with local organisations may face relates to data security requirements, particularly where the data concerns personal data. It is common for organisations seeking to engage third-party IT service providers to enter into a written data processing agreement but where the former acts as a data user

and the service provider is a data processor, the organisation, as the data user, must comply with the data security requirements under the PDPA. This includes ensuring that data processors (eg, the third-party service providers that process personal data on its behalf) provide sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and that reasonable steps are taken to ensure compliance with said measures. The Security Standard in the PDP Standard sets out certain security-related measures that the organisations must comply with, which includes binding a third party with a contract for operating and carrying out the personal data processing activities. Thus, in order to comply with their obligations under the PDPA and the PDP Standard, the organisations may require certain security measures to be put in place and these requirements may be imposed through their IT service agreements with other organisations. The organisations may also include the relevant warranty and indemnity provisions in such agreements.

Note that organisations that are not established in Malaysia but are considered to be "data users" and which use equipment in Malaysia for processing personal data, other than for the purposes of transit through Malaysia, are also required to comply with the PDPA requirements.

Sector-Specific Requirements

There may be other requirements or considerations depending on the particular facts. Where the IT service agreement is with an organisation in a regulated industry, the organisation should be aware that there may be other regulations or guidelines that such organisation may be subject to. For example, FIs in Malaysia are subject to guidelines issued by the BNM and some of the BNM's Guidelines, in particular, the Risk Management in Technology Guidelines, set out certain requirements concerning engaging third-party service providers. For instance, where an FI's IT system is managed by third-party service providers, the FI is required to ensure, including by way of contractual obligations, that the relevant third-party service providers will give sufficient notice before any changes that may impact the IT system are undertaken. There are also requirements on what a service-level agreement, which must be established by the requisite FI, must contain. Furthermore, an FI or financial service provider may be required to include specific provisions in its contract with the organisation and certain contracts/arrangements may require approval from the BNM, pursuant to the requirements under the relevant BNM Guidelines. Other BNM Guidelines include its Outsourcing Guidelines and its Management of Customer Information and Permitted Disclosures Guidelines.

Data Localisation

Despite the present lack of a general data localisation requirement under the PDPA, there may be data localisation requirements depending on the specific data in question or the industry, such as for e-money issuers storing sensitive customer information.

There are, however, restrictions concerning the cross-border transfer of data (see **6. Key Data Protection Principles**). Thus, if IT service agreements involve the transfer of personal data outside Malaysia (eg, to store the data overseas), the organisations can only do so in line with the requirements of the PDPA, while the IT service providers should ensure that such transfer by the organisation is compliant with the PDPA.

6. KEY DATA PROTECTION PRINCIPLES

6.1 Core Rules for Individual/Company Data

Core Rules Regarding Data Protection

The general PDPA framework in Malaysia is premised on the following data protection principles.

General Principle

A data user is prohibited from processing a data subject's personal data except where consent has been obtained from the data subject or where an exception applies, eg, the processing is necessary for the performance of the contract to which the data subject is party or compliance with any legal obligation of which the data user is the subject, other than a contractual obligation, etc. The General Principle also sets out certain parameters for the processing of personal data. It provides that personal data will not be processed unless:

- it is for a lawful purpose directly related to the activity of the data user;
- it is necessary for, or directly related to, that purpose; and
- the data is adequate and not excessive for that purpose.

For sensitive personal data, "explicit consent" must be obtained from the data subject to process such data, unless other exceptions apply.

Notice and Choice Principle

The PDPA requires a data user to inform a data subject by written notice of certain prescribed matters, namely:

- that the personal data of the data subject is being processed and a description of the data;
- the purposes for which the personal data is being collected and further processed;
- any information available to the data user as to the source of that personal data;
- the data subject's right to request access to and correction of the personal data and the contact particulars of the data user in the event of any enquiries or complaints;
- the class of third parties to whom the data is or may be disclosed;
- the choices and means offered to a data subject to limit the processing of the data; and
- whether it is obligatory or voluntary for the data subject to supply data, and if obligatory, the consequences of not doing so.

It is mandatory under the PDPA that the written notice (usually issued in the form of a data protection notice or privacy policy) is provided in both English and the national language (Malay).

Disclosure Principle

The PDPA prohibits the disclosure of personal data, without the data subject's consent:

- for any purpose other than that for which the data was disclosed at the time of collection, or a purpose directly related to it; and
- to any party other than a third party of the class notified by the data user.

Security Principle

The PDPA imposes obligations on the data user to take steps to protect the personal data during its processing from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Retention Principle

Personal data must not be kept longer than necessary for the fulfilment of the purpose for which it was processed. The data user has a duty to take reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is

no longer required for the purpose for which it was processed.

Data Integrity Principle

The data user must take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date, having regard to the purpose (and any directly related purpose) for which it was collected and processed.

Access Principle

The data subject must be given the right to access their own data and to correct the same where the personal data is inaccurate, incomplete, misleading or outdated. The PDPA provides grounds, however, on which the data user may refuse to comply with a data access or data correction request by the data subject.

Each principle above is subject to certain exceptions and conditions. Furthermore, in relation to the security and retention of data, and data integrity principles, specific standards are also set out in the PDP Standard for each of these principles.

Industry Codes of Practice

The Personal Data Protection Commissioner ("PDP Commissioner") has also registered several industry codes of practice such as for the banking and financial sector, utilities (electricity) sector, insurance and takaful industries, and the communications sector.

Registration of Data Users

The Personal Data Protection (Class of Data Users) Order 2013 sets out the categories of data users which are required to be registered with the PDP Commissioner, eg, banking and FIs, insurance, communications, education, services (eg, legal, accountancy, business consultancy, engineering, architecture, employment agencies, retail and wholesale).

Distinction between Companies/Individuals

The PDPA does not make a distinction between companies and individuals, as the PDPA applies to any person who processes or has control over the processing of personal data, ie, the "data user", and any individuals who are referred to as "data subjects" under the PDPA. The PDPA does not specifically distinguish or exclude business/B2B data, and the requirements under the PDPA will apply if such data consists of "personal data".

General Processing of Data

The PDPA regulates the processing of "personal data" in commercial transactions, and "processing" is broadly defined to cover a wide range of activities, including using, disseminating, collecting, recording, and/or storing of personal data.

Processing of Personal Data

Data processors

A "data processor" is defined in the PDPA as any person, other than an employee of the data user, who processes personal data solely on behalf of the data user, and does not process personal data for their own purposes. Data processors are not directly obliged under the PDPA, as the provisions are predominantly imposed on data users.

Where the data processing is carried out by a data processor on behalf of a data user, the data user must ensure that the data processor:

- provides sufficient guarantees in respect of the technical and organisational security measures governing the processing; and
- takes reasonable steps to ensure compliance with these measures.

Furthermore, the Security Standard under the PDP Standard requires a data user to bind a third party appointed by the data user with a

contract for operating and carrying out personal data processing activities.

Cross-border transfers

The PDPA generally prohibits the transfer of personal data out of Malaysia, except when it is to a permitted place (no permitted place has been gazetted at present, although a proposed whitelist has been issued, but not yet passed as operative law), or where certain exceptions apply, eg, consent has been obtained, the transfer is necessary for the performance of a contract between the data subject and the data user, or the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be processed in that place in any manner which, if that place is Malaysia, would be in contravention of the PDPA (among other exceptions).

Non-application of the PDPA

The PDPA does not apply to personal data processed outside Malaysia, unless the data is intended to be further processed in Malaysia, and it also does not apply to a data user who is not established in Malaysia, unless that person uses equipment in Malaysia to process the personal data, other than for the purpose of transit through Malaysia.

The Malaysian federal and state governments are also exempted from application of the PDPA, as well as any information processed for the purposes of a credit-reporting business under the Credit Reporting Agencies Act 2010.

Enforcement

The PDP Commissioner is the data protection authority in Malaysia. Breaches of data protection law can lead to administrative sanctions and criminal penalties. Depending on the nature of the offence, contravening the PDPA may lead to a maximum fine of MYR500,000 and/or an imprisonment term of up to three years although certain offences are compoundable, which may allow reduced penalties. There is no multiplier on penalties linked to economic loss.

To date, enforcement actions have been largely low to moderate, mainly in the form of monetary penalties imposed on entities in various sectors for offences such as failure to register as a data user, failure to obtain the requisite consent from the data subject, and data breach. The highest fines imposed thus far amounted to no more than MYR10,000.

Proposed amendments to the PDPA

In February 2020, the PDP Commissioner issued a Public Consultation Paper No 01/2020 – Review of Personal Data Protection Act 2010 ("PDP Public Consultation Paper 2020") which sets out certain proposed improvements to the PDPA to take into consideration the emerging issues on personal data protection impacting both data users and data subjects from an economic, social and technological aspect. The proposals include:

- introducing provisions on the right to data portability;
- mandatory appointment of data protection officers (DPOs) and corresponding guidelines on DPOs;
- mandatory data breach notification and corresponding guidelines on the mechanism for reporting of data breaches;
- amendment to cross-border transfer provisions;
- obligations on privacy by design and corresponding guidelines;
- expansion of data subject rights, particularly the right of data subjects to be informed when their personal data has been disclosed to a third party;
- introduction of civil rights of action;

- extension of the PDPA to personal data collected from non-commercial transactions; and
- extending the application of the PDPA to data users outside Malaysia who monitor and carry out profiling of Malaysian data subjects.

However, whether the above proposals will mature into official law remains unclear.

7. MONITORING AND LIMITING OF EMPLOYEE USE OF COMPUTER RESOURCES

7.1 Key Restrictions

Employers can monitor their employees at the workplace as well as their use of company computer resources, as there are no specific restrictions in place under Malaysian law on monitoring or limiting the use of company computer resources by employees. Such restrictions, if any, may be set out in employment agreements, employee handbooks, company policies and codes of conduct.

Application of the PDPA

However, since monitoring activities conducted by employers would likely involve the collection, storage and processing of the personal data of its employees, the PDPA, would apply. In general, monitoring the activities or use of computer resources by employees would be permitted as long as this is compliant with the requirements under the PDPA, eg, consent, notice, security, retention, data integrity, etc.

Obtaining consent

In order to conduct the monitoring activities, employers would first have to obtain the requisite consent from employees to process their data in relation to the monitoring activities unless there is an applicable exception, such as where the processing of personal data is necessary for the performance of a contract to which the employee is a party (eg, the employment contract) or for compliance with any non-contractual legal obligation which the employer is subject to. It is advisable to obtain express written consent in relation to such monitoring activities, particularly since there is a risk that sensitive personal data will also be processed.

Processing data

Furthermore, the personal data involved in the monitoring activities can only be processed where:

- the data is processed for a lawful purpose directly related to the employer's activities;
- such processing is necessary for or directly related to that purpose; and
- the personal data is adequate but not excessive in relation to that purpose.

The PDPA also requires employers to give notice or inform employees about certain prescribed information, which includes the fact that their personal data is being processed, the description of such personal data, and the purposes for which their personal data is being or is to be collected and further processed (eg, for monitoring activities). This is typically done by way of a privacy policy or notice and employers can either include the information concerning the monitoring activities in a general employee privacy policy/notice or in a separate policy/notice.

PDP Standard compliance

Employers should also ensure that their monitoring practices are compliant with the PDP Standard, in relation to measures pertaining to data security, data retention and data integrity.

Application of Other Laws

The employer should also refrain from monitoring communications and accessing content that

are evidently personal. Aside from the requirements of the PDPA, other laws may come into play depending on the facts, eg, if the monitoring activities include monitoring of personal communications or access to content on a personal device that connects with the company's computer resources, it may amount to unauthorised interception of communications or unauthorised access to computer material under the CMA and CCA. That said, whether consent suffices for the purposes of the CMA or the CCA has not been tested in court.

8. SCOPE OF TELECOMMUNICATIONS REGIME

8.1 Scope of Telecommunications Rules and Approval Requirements

Regulation of the Telecommunications Sector

The regulatory and licensing framework under the CMA is sufficiently broad to cover most technological applications even if there are no specific references to individual applications. For instance, local regulations make specific references to IP telephony and messaging services but not to RFID tags, however, all would be governed by the CMA. Service-specific issues may also be covered under various regulations, guidelines, technical codes and other voluntary codes issued by MCMC and/or other industry forums.

Licensing

Under the current telecommunications regime, there are four categories of licensable activities.

- Network Facilities Provider (NFP): for the provision of network facilities such as infrastructure, eg, satellite earth stations, fixed links and cables.
- Network Service Provider (NSP): for the provision of network services for basic connectivity and bandwidth to support a variety of applications, eg, switching services, bandwidth services, access applications service, gateway services and cellular mobile services.
- Applications Service Provider (ASP): for the provision of particular functions such as voice services, data services, content-based services, electronic commerce and other transmission services. Applications services are essentially the functions or capabilities which are delivered to end-users. Examples include PSTN telephony, public cellular services, IP telephony, public switched data services, directory services, internet access services and messaging services.
- Content Applications Service Provider (CASP): for the provision of application services which provide content, such as satellite and subscription broadcasting.

Technologies such as Voice over Internet Protocol (VoIP) and instant messaging may be considered as licensable applications services, in particular, under the categories of IP telephony and messaging services, thus requiring an ASP licence, although this still depends on the specific facts and whether there are applicable exceptions. At present, VoIP services that operate solely on the internet and messaging services where the sending and receiving of such communications are conducted entirely on the internet do not generally require a licence.

In respect of provision of VoIP as a service, "IP telephony" is defined by the Communications and Multimedia (Licensing) Regulations 2000 ("Licensing Regulations") as an "application service involving a multi-stage call set-up that involves a circuit switched to a packet switched interface". MCMC's Guideline on the Provisioning of VoIP Services expressly states that "the provision of PC to PC based internet telephony is not subject to licensing".

A "messaging service" is defined under MCMC's Licensing Guidebook as "an applications service which involves the storage or forwarding of a message in multimedia form whereby the message is first routed through a central management centre before it is forwarded to the addressee".

Spectrum Assignment

Aside from telecommunications licences, the use of spectrum (the airwaves) is regulated and the assignment of spectrum is required in order to use any part of the spectrum. The use of the spectrum is prohibited without the following.

- Spectrum assignment (SA): SA confers rights on a person to use one or more specified frequency bands for any purpose consistent with the assignment conditions set by MCMC.
- Apparatus assignment (AA): AA confers rights on a person to use the spectrum to operate a network facility of a specified kind at a specified frequency at a specified frequency band or bands.
- Class assignment (CA): CA confers rights on any person to use the frequency(ies) for a list of devices. The usage of devices under CA is subject to conditions provided in the CA issued under Section 169 of the CMA. A CA is valid until it is cancelled by MCMC.

If the technology or device falls under any of the Schedules under the CA No 1 of 2021, and use of the same complies with the requirements (including assignment conditions under the CA No 1 of 2021), no fees or application will be required.

Taking the provision of radio frequency devices (RFID) as an example, the class assignment and conditions for use of such technology or device are as specified in the Fifteenth Schedule of CA No 1 of 2021.

The devices must also be certified by MCMC or its registered certifying agency (ie, SIRIM).

Other Issues

Aside from the licensing and spectrum requirements above, there may potentially be other issues, like numbering requirements, technical standards, etc, depending on the specific facts and services.

Procedure and Cost

Licences for the licensable activities above may be issued either as "individual" or "class" licences, except for ASP licences which are only issued as class licences. An individual licence imposes a high degree of regulatory control which is for a specified person to conduct a specified activity and may include special conditions. Individual licences must be applied for and they are granted by the Minister of Communications and Multimedia. A class licence, on the other hand, is a "light-handed" form of regulation designed for easy market access and merely requires registration.

In terms of eligibility, the holders of an individual licence must be locally incorporated companies, while the holders of a class licence can be a locally incorporated company, local partnership, local sole proprietorship, or Malaysian residents. Further details concerning the application procedure and information required for such licences can be found in MCMC's Licensing Guidebook.

As for fees, the applicable fees for individual licences are as follows:

- application fee – MYR10,000 per licence (non-refundable);
- approval fee – MYR50,000 per licence; and
- annual licence fee – 0.5% of gross annual turnover or MYR50,000 (per licence), whichever is higher.

Meanwhile, for class licences, there is a registration fee of MYR2,500.

For spectrum, an SA application can only be submitted to MCMC when an Applicant Information Package (AIP) is issued, while for an AA application, the applicable fees comprise fixed fees, determined by the type of apparatus, and variable fees, based on the size of bandwidth use, and the application fee is MYR60 per application. The procedure and relevant fees can be found on MCMC's website and in the Guidelines for Apparatus Assignment.

9. AUDIO-VISUAL SERVICES AND VIDEO CHANNELS

9.1 Audio-Visual Service Requirements and Applicability

Regulation of the Media Sector

In Malaysia, content is governed by a host of laws depending on the type of content. Online content/content in the networked medium, which would include video channels, is primarily under the purview of MCMC, which also regulates licensing requirements for the provision of content in general. Specifically on censorship, the Film Censorship Board (FCB) regulates traditional media outlets and content on TV and in cinemas. The National Film Development Corporation Malaysia ("FINAS") has prerogative over film production, distribution and exhibition activities in Malaysia. Note that the likelihood of enforcement by FINAS and FCB may differ for over-the-top content, including video-sharing platform services.

Licensing Requirements – CMA

Under the CMA, providers of content applications services are required to obtain a CASP licence unless specifically exempted under the CMA. The CMA provides exemptions from licensing requirements for providers of "closed" content applications services, ie, services which are not accessible to the general public, and "incidental" content applications services, ie, services that provide content in a manner entirely incidental to the service provided. Additionally, internet content applications services (such as over-the-top services and online video-sharing platforms) are also exempted under the Communications and Multimedia (Licensing) (Exemption) Order 2000.

CASP licences may be issued as either individual licences or class licences (see **8. Scope of Telecommunications Regime**). CASPs that fall within the following criteria are likely to require an individual licence, on the basis that the content:

- is made available to the general public and is likely to be of broad appeal; and
- can be received by commonly available consumer equipment or is likely to exert a high degree of influence in shaping community views in Malaysia.

CASP individual licences are typically required for entities involved in the traditional broadcasting industry, such as terrestrial radio broadcasting, satellite broadcasting, terrestrial free-to-air TV, and subscription broadcasting. On the other hand, CASPs providing limited content applications services are not required to hold an individual licence and are exempted from the requirement to be licensed unless a class licence is applicable. A CASP of a limited content applications service is regulated by a class licence if it falls within the following categories:

- a content applications service of limited appeal or which is targeted at a special interest group and available through subscription by persons using equipment specifically designed for receiving the said service;

- a content applications service restricted to a particular geographic area;
- a content applications service for distance-learning purposes; or
- a content applications service specifically linked to or associated with a sporting, cultural or other one-off event.

As an industry regulated under the CMA, licences for the provision of content applications services are subject to the same fees and eligibility requirements as telecommunications services, and the applicable fees and eligibility requirements would depend on whether the licence is an individual licence or class licence (see **8. Scope of Telecommunications Regime**). Applications for licences are to be made to MCMC in the prescribed forms.

Other Licences/Approvals

Depending on the facts, additional licensing requirements may apply. For example, the production, distribution or exhibition of films may require a licence from FINAS. Such films may also require the approval of the FCB.

Content Requirements and Restrictions

As set out above, content is subject to a host of laws depending on the type of content, the main laws being:

- the CMA;
- the Printing Presses and Publications Act 1984;
- the FCA;
- the Sedition Act 1948;
- the Penal Code;
- sharia; and
- advertisement laws, codes and guidelines.

For example, the CMA generally prohibits the provision of content that is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person via a content applications service, and content that is deemed seditious will contravene the Sedition Act. Additional laws may also apply depending on the specific facts, such as the Copyright Act for content that infringes copyright.

To aid the regulation of the content industry, the Communications and Multimedia Content Forum ("Content Forum") issued the Malaysian Communications and Multimedia Content Code ("Content Code"). The Content Code contains obligations and restrictions relating to content, and contains guidelines for a variety of different content platforms, including advertising guidelines, specific broadcasting guidelines, and specific online guidelines.

Of relevance to providers of video-sharing platform services, the Content Code stipulates that providers of access to content who have neither control over the composition of such content, nor any knowledge of such content, are deemed innocent carriers, and are not responsible for the content provided.

The Content Forum recently issued a public consultation paper on proposed amendments to the Content Code. Notable proposed amendments include the lifting of the prohibition on advertising alcoholic drinks over electronic mediums, and the introduction of specific guidelines for public service announcements by licensed gambling or betting companies.

10. ENCRYPTION REQUIREMENTS

10.1 Legal Requirements and Exemptions

While there are no statutes that specifically govern encryption or the use of encryption technology in Malaysia, there are existing laws and

regulations which may apply to various facets of encryption, and certain industries have issued specific guidance that touches on the use of encryption.

PDPA

While the PDPA does not mandate/require the use of encryption in systems which process personal data, the Security Principle generally requires data users to take "practical steps" to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction (see **6. Key Data Protection Principles**).

Although these "practical steps" are not defined in the PDPA or its subsidiary legislation, the use of encryption by organisations in securing their systems would no doubt be a valuable security measure. Notably, the Personal Data Protection Codes of Practice, issued by the PDP Commissioner for certain regulated industries, such as the telecommunications and financial industries, recommend encryption as a measure to adhere to the security principle of the PDPA.

Furthermore, the PDP Public Consultation Paper 2020 sought to introduce, among other things, a duty to report data breaches to the PDP Commissioner and an endpoint security policy requiring the use of technology such as encryption to secure personal data. Organisations are therefore further encouraged to implement robust security systems, which involve the use of encryption technology, to ensure their personal data systems are securely protected.

Strategic Trade Laws

The use of encryption in a particular device or system may come within the definition of "strategic items" under the Strategic Trade Act 2010 (STA) and the Strategic Trade (Strategic Items) Order 2010 (STO).

Under the STO, unless any of the exemptions apply, the exportation of strategic items, such as dual-use encryption hardware, software and technology, are restricted in Malaysia. Dual-use encryption items refer to items capable of being used for a non-military and a military purpose or in relation to the proliferation of weapons of mass destruction, and includes the technology necessary for the development, production or use of any dual-use items. Export of strategic items to "prohibited end-users" as prescribed in the Strategic Trade (Restricted End-Users and Prohibited End-Users) Order 2010 is absolutely prohibited, while the export of strategic items to "restricted end-users" requires a special permit. Such restrictions also extend to intangible transfers of controlled technology.

However, there are a number of exclusions to export controls on dual-use encryption hardware, software and technology, including exclusions for products which accompany their user for the user's personal use, and certain cryptographic items intended for sale to general consumers.

The importation of strategic items, on the other hand, is not restricted in Malaysia. However, imports of IT/telecommunications equipment (including any embedded encryption software and hardware) requires both an import licence and type approval from SIRIM.

Sector-Specific and Data-Specific Requirements

Depending on the specific sector and the type of data, there may be additional requirements pertaining to the use of encryption technologies.

- In the financial services industry, pursuant to the Policy Document on Risk Management in Technology issued by the BNM, the use of encryption technologies is mandatory for FIs when dealing with important data and

information. Pursuant to the policy document, FIs are required, among other requirements, to establish a robust and resilient cryptography policy to promote the adoption of strong cryptographic controls for protection of important data and information. The policy document further requires that FIs conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation, and non-repudiation of information.

- In the telecommunications sector, encryption technologies are referenced in a number of technical codes, including the Technical Code on Information and Network Security – Requirements, which specifies, among other things, the use of cryptography to protect the confidentiality, authenticity and integrity of information.

The Malaysian government has also developed a portfolio of national, trusted cryptographic algorithms via its MySEAL programme, a multi-year effort which evaluates and thereafter recommends cryptographic algorithms. Certain information, eg, official secrets as defined in the Official Secrets Act and information of national importance, may be subject to stricter requirements.

Other Laws/Regulations

Organisations using encryption should be aware of other laws in Malaysia that enable law enforcement authorities to seek disclosure of encryption keys and to gain access to encrypted data, including:

- the Anti-Trafficking and Anti-Smuggling of Migrants Act 2007;
- the CCA;
- the PDPA;
- the STA;
- the CMA;
- the Criminal Procedure Code; and
- the Digital Signature Act.

For instance, under the CCA, a police officer or an authorised officer conducting a search must be given access to computerised data stored in a computer which may include encrypted data. Similarly, under the CMA, an authorised officer making an investigation must be given access to computerised data and such data may include encryption and decryption codes. Provisions of this nature are also found in the PDPA and the STA, along with numerous other laws in Malaysia.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

The Malaysian government introduced numerous measures and initiatives in response to COVID-19, primarily via the Temporary Measures for Reducing the Impact of Coronavirus Disease 2019 (COVID-19) Act 2020 ("COVID-19 Act"), the Prevention and Control of Infectious Diseases Act 1988 ("Infectious Diseases Act"), and the various emergency ordinances, including but not limited to the Emergency (Essential Powers) (No 2) Ordinance 2021 (the "Ordinance"). While these laws are not TMT-specific, they afford considerable flexibility to the government in devising appropriate responses to problems stemming from the pandemic.

Notably, via the Infectious Diseases Act, the government placed Malaysia under a lockdown with multiple phases to curb the spread of COVID-19, and has now placed the country under a National Recovery Plan (the "Plan"), with standard operating procedures (both general and sector-specific) which vary depending on the phase of the Plan Malaysia is currently in.

COVID-19 Act

The COVID-19 Act introduced a number of measures to provide relief to parties affected by COVID-19. While some of the measures under the COVID-19 Act are no longer in operation, others continue via orders gazetted to extend their period of operation. The following are examples of some of these measures.

- Up until 22 October 2022, parties to certain categories of contracts (eg, professional services and construction contracts) may not exercise their rights under the contract due to the inability of the other party to perform their contractual obligation(s) as a result of measures taken by the government to control or prevent the spread of COVID-19.
- Limitation periods for actions under contract and tort, for actions to enforce an award or recognisance, and for actions to recover any sum recoverable by virtue of any written law, which expired during the period 18 March 2020 to 31 August 2020, were extended to 31 December 2020.
- Up until 31 December 2020, credit facility providers were not permitted to commence legal proceedings to recover outstanding amounts payable under credit sale agreements entered into before 18 March 2020.

The Ordinance

The Ordinance came into force in March 2021 as an effort by the government to curb the spread of misinformation and "fake news" regarding the pandemic or the proclamation of the emergency itself. Notably, the Ordinance criminalised the creation, publication, or dissemination of fake news and indirectly imposed liability on media organisations or social media platforms if they failed to remove publications containing content deemed as fake news within 24 hours.

A motion for the Ordinance to be revoked, along with its sister emergency ordinances, was approved by the Malaysian House of Representatives on 8 December 2021.

Relief Programmes

The BNM has also created and enhanced existing financing facilities to support the recovery of SMEs affected by the pandemic. The relevant facilities for the TMT sector are the High Tech Facility – National Investment Aspirations (HTF-NIA) and the SME Automation and Digitalisation Facility (ADF).

The HTF-NIA was established to finance affected hi-tech and innovation-driven SMEs that are aligned with the long-term development goals in Malaysia's National Investment Aspirations. Through the HTF-NIA, eligible SMEs may be granted up to MYR1 million for working capital or up to MYR5 million for capital expenditure, or a combination of both. The facility under the HTF-NIA may be granted for up to seven years and is available until 30 June 2022 or the full utilisation of the facility, whichever is earlier.

The ADF, on the other hand, is focused on incentivising SMEs to automate processes and digitalise operations to improve productivity and efficiency. Eligible SMEs may be given an amount up to MYR3 million for a period of up to ten years. Like the HTF-NIA, the ADF was made available until 30 June 2022 or the full utilisation of the facility, whichever is earlier.

Other Initiatives

COVID-19 has accelerated the need to develop Malaysia's digital economy, resulting in the introduction of the Malaysia Digital Economy Blueprint by the Malaysian government, which will run from 2021 until 2030 and which endeavours:

- to introduce the "Digital-First" programme to encourage increased usage of cloud services by federal and state bodies;

- to review existing laws, including the PDPA, Digital Signature Act, and Official Secrets Act;
- to increase the capacity and capability of related enforcement agencies, including through standards and certification; and
- to improve cross-border data transfer mechanisms in the PDPA and international trade policies.

While some of the main developments have been highlighted above, there are other examples of government action which have not been addressed, some of which are no longer in effect. Examples include the introduction of moratoriums and tax incentives.

Skrine is a leading legal firm in Malaysia with a global reputation and a wide range of highly regarded practice groups to meet the increasingly diverse needs of its clients. As one of the largest legal firms in Malaysia, Skrine is committed to the development of legal minds and the improvement of the community in which it exists. In an increasingly borderless and competitive world, where the law is challenged in new ways daily, Skrine remains steadfast in its founding principles: wisdom, fortitude and ingenuity. Charmayne Ong leads the firm's TMT practice, which currently consists of six lawyers. The team has vast experience in providing regulatory advice on various trending telecommunications issues such as over-the-top (OTT) service offerings, establishment of data centres for cloud computing services, and leasing of sub-sea and terrestrial fibres. It also advises clients on regulatory compliance queries and assists them in obtaining regulatory approvals and licences, such as spectrum assignments and telecommunications licences.

AUTHORS

Charmayne Ong heads both the IP practice and the TMT practice at Skrine. As a leading figure in IP and TMT legal advisory and compliance, Charmayne has extensive experience and has worked with regulators, public institutions and companies of all sizes. Charmayne manages the registration of, and general advisory and drafting work relating to, the classic forms of IP rights. She also regularly deals with regulators and advises clients who provide technology and telecommunications, such as satellite, internet and on-demand content services, on complex regulatory compliance and licensing matters. She is the Malaysian member of the Global Leaders Forum (TMT practice) and a member of the Federation of Malaysian Manufacturers (for IP and TMT).

Natalie Lim is a partner in the IP practice at Skrine and has a strong focus on TMT and data protection. She regularly advises domestic and international clients in the TMT sector on various regulatory matters concerning their infrastructure and services such as satellite communications, fibre and terrestrial wireless connectivity, cloud services, OTT services, and encryption. Natalie also advises multinational and local companies on data protection issues, including compliance with data protection laws, as well as drafting the necessary documents and assisting with registration. Her expertise includes advising on, drafting and negotiating IP licence and assignment agreements as well as technology agreements, such as outsourcing, licensing, development and systems integration.

Jillian Chia leads the privacy and data protection practice at Skrine and is also part of the firm's TMT practice. She focuses on advising local and multinational companies on data protection and privacy issues. Jillian's experience in this area includes reviewing and drafting relevant documentation such as privacy policies, data processor agreements and data transfer agreements, as well as bringing her clients' internal practices in line with the requirements of privacy and data protection laws. She is also well versed in the TMT industry and advises a wide range of global telecommunications and technology companies on their investments and service offerings in Malaysia. In addition, she handles registration of industrial designs and general advisory work relating to IP rights.

Skrine

Level 8, Wisma UOA Damansara
50 Jalan Dungun
Damansara Heights
50490
Kuala Lumpur
Malaysia

Tel: + 603 2081 3999
Fax: + 603 2094 3211
Email: skrine@skrine.com
Web: www.skrine.com

Trends and Developments

Contributed by:
Charmayne Ong, Natalie Lim and Jillian Chia
Skrine see p.28

Introduction

With the ever-present shadow cast by the pandemic, a reflection on the events of the past 12 months seems to be nothing short of a habitual exercise; however, 2021 may yet be remembered as a year of pivotal developments in the TMT landscape in Malaysia. The following are some of the pertinent developments that have captured the regulatory headlines this year.

Rolling Out 5G Nationwide

Like many other countries, Malaysia has taken proactive measures in its efforts to adequately prepare the country to face the far-reaching changes of the digital age and the Industrial Revolution 4.0 through the adoption of 5G technology. This past year, 2021, was highly significant in this respect considering the developments that have helped to bring about 5G implementation in Malaysia. In February 2021, the then-prime minister of Malaysia announced that, as part of the government's MyDIGITAL initiative, the implementation of 5G in Malaysia would be undertaken by a government-owned special purpose vehicle (SPV).

In the same month, the Ministry of Finance announced that Digital Nasional Berhad (DNB), a government-owned SPV, would be the sole entity undertaking the deployment of the 5G infrastructure and network in Malaysia, therefore granting DNB a monopoly over the provision of wholesale 5G services in Malaysia. In May 2021, the Minister of Communications and Multimedia then issued a Ministerial Direction confirming this. Foreseeing a potential backlash over this decision, the Malaysian Communications and Multimedia Commission (MCMC) has assured industry players and the public that it is committed to ensuring that local telecommunications operators and other interested parties are able to secure access to DNB's 5G services on equitable and non-discriminatory terms through a number of legal mechanisms available to it.

In furtherance of its objective to effectively regulate DNB's provision of wholesale 5G services, in December 2021, MCMC published the Commission Determination on Access List, Determination No 6 of 2021 ("Access List"), which sets out a list of facilities and services to which access must be provided in accordance with predetermined standards and obligations, including the obligation to provide access on an equitable and non-discriminatory basis. The Access List includes the provision of two models of 5G access:

- 5G Standalone Access; and
- 4G Evolved Packet Core with 5G Radio Access Network Access.

In accordance with the Access List, the provision of access to each model must be compliant with the Release 15 standards set by the 3rd Generation Partnership Project (3GPP), including any updates to the standard, and must provide all necessary technical capabilities to enable the provision of certain services to end-users, such as mobile broadband services. The introduction of 5G services to the Access List marks a significant milestone for 5G regulation in Malaysia, as it sets the foundation for further regulation via other legal instruments.

In the future, we may expect further quality-of-service requirements in respect of 5G services as MCMC prepares to update the mandatory

standards on access, which set out the basis on which access to the facilities/services listed in the Access List are to be provided, to include specific obligations and standards for the provision of access to 5G services. The update is expected to come into force some time in 2022, and interested parties are advised to keep an eye out for its inevitable arrival.

In connection with these developments, MCMC has also released technical codes containing requirements covering 5G user equipment (eg, portable equipment and modems), 5G base stations and cellular booster equipment, for the purpose of certifying communications equipment pursuant to the Communications and Multimedia Act 1998 (CMA). While much has unfolded in the 5G landscape so far, further developments in the implementation of 5G are expected, and interested parties are advised to keep watch for these.

Licensing Cloud Service Providers

Over the past few years, Malaysian policymakers have been increasingly receptive towards cloud services. The "Cloud First" Strategy, first introduced in October 2017, encouraged the use of cloud computing in the public sector, with the aim of achieving 50% cloud adoption by 2025. This was cemented by the development of the "Cloud First" policy in the National Cloud Services Hub and Data Center Policy Framework, which requires the public sector to prioritise the use of cloud computing. More recently, the Malaysian government launched the MyDIGITAL Blueprint which, among other things, expressed the government's intention to raise the target of public-sector cloud adoption to 80% by 2022 as well as boost the capabilities of domestic data centre companies to provide high-end cloud computing services.

On 16 October 2021, MCMC, in acknowledgement of the increased reliance on cloud services in line with the MyDIGITAL Blueprint initiatives and "Cloud First" policy, issued an advisory notice expressing its intention to adopt light-touch regulation on cloud service providers, citing concerns about data safety and trust in the light of the high levels of cloud adoption among consumers. As a result, effective from 1 January 2022, cloud service providers with a local presence which provide cloud services to end users in Malaysia are required to obtain an Applications Service Provider Class (ASP(C)) licence, which forms one of the licence categories currently set out under the CMA. This subjects the cloud service provider to certain standard licence conditions, such as the requirement to comply with consumer codes registered under the CMA, and special conditions which may be issued on a case-by-case basis.

Despite the introduction of a licensing regime, interested parties should note that the decision by MCMC to issue ASP(C) licences to cloud service providers is predicated on MCMC's desire to regulate cloud services using a light-touch approach, stemming from its objective to promote industry growth and development in the cloud services environment. To illustrate, holders of an ASP(C) licence will not be subject to any foreign equity restrictions, whereas holders of other licence types, namely individual licences, are typically subject to such foreign equity restrictions.

Realising Fixed Number Portability (FNP)

Since 2016, service providers in the communications industry have been vocal in expressing their interest and support for FNP implementation in Malaysia, which has only been compounded following consultation sessions between service providers and MCMC in 2018. In response to this, MCMC issued a public consultation in December 2020 seeking views on the implementation of FNP, namely, the most appropriate and effective FNP service(s) and technical solution(s)

to implement, as well as inquiring how the process should be administered, and the appropriate method to expedite the implementation of FNP in a simple and inexpensive way.

It was MCMC's understanding that with the implementation of FNP, a potentially significant barrier to customer choice and switching would be removed, thus facilitating more effective competition in the fixed telephony market. Given the increase in bundled services, it was also hoped the implementation of FNP would exert a wider influence on competition across the telecommunications market. In July 2021, MCMC published its report on the inquiry as the conclusion to this public consultation exercise.

In brief, MCMC indicated in the report its support for service provider portability for FNP and sees FNP as a means to introduce a more competitive landscape to the fixed service market in Malaysia, thus providing increased benefits to consumers. The report also indicates that MCMC plans to implement location portability within the same area code by the end of 2022.

Revamping the Content Code

The regulation of content over a networked medium has also seen some changes recently. Having only released the existing Content Code last year, the Communications and Multimedia Content Forum of Malaysia (CMCF) has commenced a new public consultation exercise on the Content Code, which contains guidelines and procedures for governing standards and best practices for content dissemination within the communication and multimedia industry.

The consultation was driven by the aim to address policy gaps on new content-related issues that have arisen as a result of significant changes in the industry and to provide more comprehensive and holistic guidelines and best practices for the industry while maintaining the principle of self-regulation.

Notably, the proposed Content Code introduces several provisions to cater to the growth of content within new advertisement areas. A key proposed amendment is the decision to expand the application of advertising guidelines under the current Content Code to cover influencer marketing, requiring that advertisements or marketing communications that include the involvement of third parties are clearly disclosed as being done in exchange for payment in cash or some other reciprocal arrangement in lieu of cash. There appears to be a possible degree of relaxation in the regulation of advertisements of alcoholic drinks and liquor, considering the proposed revisions to permit advertising of intoxicating liquor to be communicated over electronic based media (excluding broadcast media such as television and radio), subject to strict restrictions (eg, with clear provisions governing age).

Additionally, for advertisements by licensed gambling or betting companies, the proposed Content Code seeks to clarify that such companies are allowed to air public service announcements and corporate social responsibility campaigns provided that the messages are from their charitable arm and do not include any essence of the products or marketing elements such as the original tagline or logo.

Also notably featured were MCMC's proposals to:

- prohibit online abuse and content that incites or provokes any act of abuse and gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or abuse;
- require the delivery of content and information intended for the general public in acces-

sible formats and technologies appropriate for persons with disabilities; and
- qualify the scope of content considered indecent by permitting nude content under certain circumstances.

Contributed by: *Charmayne Ong, Natalie Lim and Jillian Chia,* ***Skrine***

Skrine is a leading legal firm in Malaysia with a global reputation and a wide range of highly regarded practice groups to meet the increasingly diverse needs of its clients. As one of the largest legal firms in Malaysia, Skrine is committed to the development of legal minds and the improvement of the community in which it exists. In an increasingly borderless and competitive world, where the law is challenged in new ways daily, Skrine remains steadfast in its founding principles: wisdom, fortitude and ingenuity. Charmayne Ong leads the firm's TMT practice, which currently consists of six lawyers. The team has vast experience in providing regulatory advice on various trending telecommunications issues such as over-the-top (OTT) service offerings, establishment of data centres for cloud computing services, and leasing of sub-sea and terrestrial fibres. It also advises clients on regulatory compliance queries and assists them in obtaining regulatory approvals and licences, such as spectrum assignments and telecommunications licences.

AUTHORS

Charmayne Ong heads both the IP practice and the TMT practice at Skrine. As a leading figure in IP and TMT legal advisory and compliance, Charmayne has extensive experience and has worked with regulators, public institutions and companies of all sizes. Charmayne manages the registration of, and general advisory and drafting work relating to, the classic forms of IP rights. She also regularly deals with regulators and advises clients who provide technology and telecommunications, such as satellite, internet and on-demand content services, on complex regulatory compliance and licensing matters. She is the Malaysian member of the Global Leaders Forum (TMT practice) and a member of the Federation of Malaysian Manufacturers (for IP and TMT).

Natalie Lim is a partner in the IP practice at Skrine and has a strong focus on TMT and data protection. She regularly advises domestic and international clients in the TMT sector on various regulatory matters concerning their infrastructure and services, such as satellite communications, fibre and terrestrial wireless connectivity, cloud services, OTT services, and encryption. Natalie also advises multinational and local companies on data protection issues, including compliance with data protection laws, as well as drafting the necessary documents and assisting with registration. Her expertise includes advising on, drafting and negotiating IP licence and assignment agreements as well as technology agreements, such as outsourcing, licensing, development and systems integration.

Jillian Chia leads the privacy and data protection practice at Skrine and is also part of the firm's TMT practice. She focuses on advising local and multinational companies on data protection and privacy issues. Jillian's experience in this area includes reviewing and drafting relevant documentation such as privacy policies, data processor agreements and data transfer agreements, as well as bringing her clients' internal practices in line with the requirements of privacy and data protection laws. She is also well versed in the TMT industry and advises a wide range of global telecommunications and technology companies on their investments and service offerings in Malaysia. In addition, she handles registration of industrial designs and general advisory work relating to IP rights.

Skrine

Level 8, Wisma UOA Damansara
50 Jalan Dungun
Damansara Heights
50490
Kuala Lumpur
Malaysia

Tel: + 603 2081 3999
Fax: + 603 2094 3211
Email: skrine@skrine.com
Web: www.skrine.com