TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS (TMT) SERIES - MALAYSIA

*This article is the third in a series exploring the Malaysian legal position with respect to various commonly asked questions in relation to the Technology, Media, and Telecommunications ("**TMT**") legal regime in Malaysia.*

In Part C of our TMT Series, we will be answering various queries pertaining to the Information Technology legal regime in Malaysia.

PART C: INFORMATION TECHNOLOGY

1. Are there any restrictions applicable to cloud-based services?

The Malaysian Communications and Multimedia Commission ("**MCMC**") has released an advisory notice titled "*Cloud Service Regulation Introduced to Increase Accountability for User Data Security and Sustainability of Services*" ("**Advisory Notice"**) and an information paper titled "*Information Paper on Regulating Cloud Services*" ("**Information Paper**"), which provide a regulatory framework for cloud-based services in Malaysia.

The Advisory Notice defines 'cloud services' broadly as *"any service made available to end users on demand via the Internet from a cloud computing provider's server".*

The Advisory Notice and Information Paper provide that providers of cloud services would need to apply for an "*Applications Service Provider*" class license ("**ASP(C)**") from the MCMC, which has a validity period of 1 year and is to be renewed annually. The provision of cloud-based services without the ASP(C) licence would constitute an offence under the Communications and Multimedia Act 1998 ("**CMA**") and would be punishable upon conviction with a fine of up to RM500,000 and/or imprisonment for up to 5 years.

It should be noted that the Advisory Notice specifies that "*persons providing the cloud services with local presence*" would need to be registered as an ASP(C) licensee. The Information Paper also elaborates on how "*local presence*" may be determined, as follows:

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my |T: +603 2201 5584

(a) *"a person that is locally incorporated/established in accordance with the relevant laws. However, a local branch of a foreign person would not fall within this category as a branch of a foreign person is still regarded as part of the said foreign person and would be inconsistent with Regulation 23 of the Communications and Multimedia (Licensing) Regulations 2000; or*

(b) *a person that is locally incorporated/established in accordance with the relevant laws and provides cloud services that originates from a foreign cloud service provider, through its local data centre. In this respect, the provisioning of the foreign cloud services would be undertaken by the local data centre which would have control over the cloud services that are being made available to the end users."*

As the regulatory framework under the Advisory Notice and Information Paper are intended to be 'light touch' approaches by the MCMC, there are no foreign equity restrictions and cloud-based service providers are also eligible for a waiver from contributing to the Universal Service Provision Fund which all CMA licensees (except for content applications services providers) are required to contribute to.

It should be noted that notwithstanding the Advisory Notice and Information Paper, cloud-based services may also be subject to other legislation depending on the nature of the cloud services provided, in particular:

(a) the MCMC in October 2018 registered a technical code on Information and Network Security – Cloud Service Provider Selection ("**CSPS Code**") which seeks to set out the requirement for network interoperability and the promotion of safety of network facilities by specifying the requirements for selecting cloud service providers for organisations in ensuring all security requirements are taken into account based on the assessment of the current environment and objectives. While compliance with the CSPS Code is not in itself mandatory for cloud service providers or organisations appointing cloud service providers, the MCMC is empowered to direct a person or a class of persons to comply with the CSPS Code. Failure to comply with such directions by the MCMC may result in a fine of up to RM200,000 being imposed;

(b) financial institutions which intend to use data services or cloud services providers outside of Malaysia to deliver cloud services are required to seek approval from BNM in accordance with BNM's Policy Document

on Outsourcing (which came into force on 1 January 2019) and BNM's Guidelines on Data Management and Management Information System Framework for Development Financial Institutions; and

(c) cloud-based service providers would fall under the purview of the Personal Data Protection Act 2010 ("**PDPA**") as "*data users*", i.e. "*a person who either alone or jointly or in common with other persons processes any personal data, or has control over or authorises the processing of any personal data*" as the act of "*processing*" has been defined in the PDPA to include "*storing of personal data*". Cloud-based service providers storing personal data using cloud-based services would have to ensure that they comply with the provisions of the PDPA.

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

Save for transactions involving powers of attorney, wills, and codicils, trusts and other negotiable instruments, the Electronic Commerce Act 2006 ("**ECA**") applies to commercial transactions conducted through electronic means.

Section 9(1) of the ECA provides that "*Where any law requires a signature of a person on a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by an electronic signature which—*

(a) is attached to or is logically associated with the electronic message;

(b) adequately identifies the person and adequately indicates the person's approval of the information to which the signature relates; and

(c) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required."

Section 9(2) of the ECA further states that "*For the purposes of paragraph (1)(c), an electronic signature is as reliable as is appropriate if—*

(a) the means of creating the electronic signature is linked to and under the control of that person only;

(b) any alteration made to the electronic signature after the time of signing is detectable; and

(c) any alteration made to that document after the time of signing is detectable."

The ECA further provides that the Digital Signature Act 1997 ("**DSA**") continues to apply to any digital signature used as an electronic signature in any commercial transaction. A digital signature is defined under the DSA as *"a transformation of a message using an asymmetric cryptosystem 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 had been altered since the transformation was made."*

Section 62(1) of the DSA specifically prescribes that:

"Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where—

(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(b) that digital signature was affixed by the signer with the intention of signing the message; and

(c) the recipient has no knowledge or notice that the signer—

(i) has breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature."

Section 66 of the DSA also provides that a certificate issued by a licensed certification authority shall be an acknowledgment of a digital signature verified by reference to the public key listed in the certificate if that digital signature is (a) verifiable by that certificate; and (b) affixed when that certification was valid.

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

The Guidelines on Information Security in ICT Outsourcing published by CyberSecurity Malaysia (an agency under the MCM) ("**Outsourcing Guidelines**") states: *"Before outsourcing, an organisation is responsible for the actions of all their staff and liable for their actions. When these same people are transferred to an outsourcer they may not change desk but their legal status has changed. They no longer are directly employed or responsible to the organisation. This causes legal, security and compliance issues that need to be addressed through the contract between the client and suppliers. This is one of the most complex areas of outsourcing and requires a specialist third party adviser."*

The Outsourcing Guidelines advise that the organization ought to ensure that security requirements and processes to protect organizational assets ought to be incorporated into the formal agreement entered into with the outsourcing supplier and upon complete performance of the outsourcing agreement, the outsourcing supplier is responsible for returning all borrowed assets and the organization should ensure that *"all assets borrowed and used by the outsourcing provider during the outsourcing project are returned promptly".*

Notwithstanding the advisory nature of the Outsourcing Guidelines, the treatment and status of employees, assets and/or third-party contracts would typically also be addressed in the outsourcing agreement and may not be automatically transferred.

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

There is no specific legislation regulating artificial intelligence ("**AI**") in Malaysia. Software programmes with a form of AI would be treated similarly to other consumer products. In the event of a malfunction, liability would be addressed by the Sale of Goods Act 1957 ("**SOGA**"), Consumer Protection Act 1999 ("**CPA**") and the law of torts, which collectively serve as a platform for product safety and consumer protection.

The Contracts Act 1950 ("**Contracts Act**"), which serves to address the rights and liabilities of parties pursuant to a contract, would be relevant in determining liability for AI malfunctions. In a contract relating to the use of an AI, provisions may be included to determine which of the parties will sustain liability arising out of AI malfunctions.

Section 68(1) of the CPA states that *"where any damage is caused wholly or partly by a defect in a product, the following persons shall be liable for the damage:*

(a) the producer of the product;

(b) the person who, by putting his name on the product or using a trade mark or other distinguishing mark in relation to the product, had held himself out of the producer of the product; and

(c) the person who has, in the course of his business, imported the product into Malaysia in order to supply it to another person."

The SOGA and the CPA impose several implied terms which cannot be excluded by contract when dealing with consumers. These include implied guarantees and conditions regarding title and lack of encumbrances, correspondence with description, satisfactory or acceptable quality, fitness for purpose, price, and repairs and spare parts. The AI software manufacturer or supplier would be liable for any malfunction that results in a breach of these mandatory implied terms, depending on the extent of non-compliance with the representations and guarantees made by the manufacturer to the supplier and the supplier to the consumer respectively regarding the AI software programme.

Manufacturers may rely on the "development of risk" defence to exonerate liability by demonstrating that apart from observing the industrial standard, the scientific and technical knowledge at the relevant time disabled any attempts of discovering the defect. However, the strict liability rule introduced in the CPA will have a significant bearing in negating the defence. Manufacturers and/or suppliers may also be found liable for AI software malfunctions under the tort of negligence.

If an AI is tasked with creating content and malfunctions by incorporating third-party works protected by copyright in such content without authorisation, the liability for such infringement pursuant to the SOGA, CPA, Contracts Act, and law of torts would accrue to the creator of the AI, subject to any contractual provisions addressing liability between the creator and the user of the AI for such infringement occasioned by the AI.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my |T: +603 2201 5584

However, with rapidly growing development of AI such as the introduction of Google Duplex, AI may no longer be a mere product, but one capable of human mimicry and potentially gaining legal personality, consciousness, personhood, authorship and autonomy. In such event, the legal position on AI would drastically change.

If you have any related questions/queries please do not hesitate to contact us:

E: general@shinassociates.com.my |T: +603 2201 5584