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

*This article is the fourth 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 D of our TMT Series, we will be answering various queries pertaining to the Cybersecurity legal regime in Malaysia.

PART D: KEY LAWS OF MALAYSIA - CYBERSECURITY

What key laws exist in terms of obligations as to the maintenance of cybersecurity?

There is currently no single legislation governing cybersecurity. In April 2019, the Malaysian government indicated that it is studying the possibility of introducing an Act on cybersecurity, however no definite timeframe has been set for its development. The current legislation applicable to cybersecurity are:

(a) Computer Crimes Act 1997 ("**CCA**"): The CCA provides for offences relating to the misuse of computers and applies if the computer, programme or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time. The act(s) of gaining unauthorized access into computers or networks, committing or facilitating the commission of further offences, unauthorized modification of the contents of any computer and/or wrongful communication are all offences under the CCA and depending on the offence, upon conviction, applicable fines range from RM25,000 to RM150,000 and/or imprisonment of 3 to 10 years.

(b) Communications and Multimedia Act 1998 ("CMA"): The CMA was enacted to provide for and to regulate the converging communications and multimedia industries and regulates network facilities, network services, applications services, content applications services and includes the prescription of the licensing framework relating to such services and the activities undertaken by licensees thereunder. Section 263(1) of the CMA prescribes that "*A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia.*" The CMA prohibits *inter alia* the fraudulent or improper use

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

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

of network facilities or network services; the use and possession of counterfeit access devices; the use of equipment or devices to obtain unauthorized access to any network services; and interception of any communications except with lawful authority.

(c) Copyright Act 1987 ("**CA**"): It is an offence under Section 36A of the CA to circumvent (or the cause or authorization thereof) of any technological protection measure that is applied to a copy of copyright work. Technological protection measure is defined as "*any technology, device or component that, in the normal course of its operation, effectively prevents or limits the doing of any act that results in an infringement of the copyright in a work*". The CA also expressly prohibits anyone from (a) designing, producing, adapting or performing for the purpose of enabling or facilitating the circumvention of technological protection measure; and (b) to manufacture, import or sell any technology or device for the purpose of circumventing any technological protection measure.

(d) Penal Code ("**PC**"): Where specific cybersecurity-related offences are not captured under the CCA, CMA or CA, the PC which codifies most criminal offences and procedures in Malaysia, may be relied on to prosecute such offences.

(e) Personal Data Protection Act 2010 ("**PDPA**"): The PDPA applies to any person who processes and has control over or authorises the processing of any "personal data" in respect of commercial transactions. There are 7 data protection principles that form the basis of protection under the PDPA, one of which is the Security Principle. Pursuant to Section 9(1) of the PDPA, a data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access of disclosure, alteration or destruction. In addition to the provisions of the PDPA, the Regulations also require data users to develop a security policy to ensure that personal data is protected from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. The Department of Personal Data Protection published the Personal Data Protection Standard which enumerates the minimum security standards for personal data processed electronically and non-electronically. The SC on 31 October 2016 also published Guidelines on Management of Cyber Risk making it mandatory for entities to have clear and comprehensive cyber policies and procedures which are commensurate with their risk profiles.

(f) Strategic Trade Act 2010 ("**STA**"): As part of Malaysia's international obligations on national security, the STA controls the export, transhipment, transit and brokering of strategic items and technology, including arms and

related materials, as well as activities that will or may facilitate the design, development, production and delivery of weapons of mass destruction. Section 7 of the STA provides that the Minister of International Trade and Industry may, by order published in the Gazette, prescribe any items as strategic items for the purposes of the STA.

(g) Other Applicable Guidelines or Regulations: The National Cyber Security Policy ("**NCSP**") was implemented by the Malaysian government with the aim to develop and establish a comprehensive programme and a series of frameworks to ensure the effectiveness of cybersecurity controls over vital assets and various sectors comprising the Critical National Information Infrastructure ("**CNII**"). While there are generally no minimum protective measures required, the Malaysian government has stipulated ISO/IEC 27001 Information Security Management Systems as the basis for information security standards and has proposed for all CNII sectors to be appropriately certified. There are also sector-specific guidelines that deal with cybersecurity in Malaysia. These include the Data Management and Management Information System Framework and Guidelines on Internet Insurance issued by the Central Bank of Malaysia.