Shearn Delamore &co.

Technology, Media & Telco Update

DECEMBER 2024

2024 Year in Review: Technology, Media & Telecommunications Laws

The year 2024 marked a transformative chapter for Malaysia, as significant legal developments reshaped the technology, media, and telecommunications ("**TMT**") landscape. These changes underscore the nation's progress in adapting to the rapidly evolving digital era and addressing the complex regulatory challenges of modern technology.

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

To further enhance digital governance, Malaysia unveiled the **National Guidelines on AI Governance & Ethics**, encouraging responsible use of artificial intelligence ("**AI**").

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

While these legal developments have profound implications for the ICT sector, their impact is broader, with laws like the Cyber Security Act 2024 and amendments to the Personal Data Protection Act 2010 applicable across industries, to safeguard data and bolster cyber security nationwide.

As 2024 draws to a close, this article reviews these pivotal developments, presented in a generally reverse chronological order, illustrating how they have reshaped the TMT and ICT legal framework and influenced governance across various sectors.

Shearn Delamore & Co
7th Floor
Wisma Hamzah Kwong-Hing,
No 1, Leboh Ampang
50100, Kuala Lumpur, Malaysia
T: 603 2027 2727
F: 603 2078 5625
info@shearndelamore.com
www.shearndelamore.com
www.linkedin.com/company/shearn-delamore-&-co

Introduction of the Data Sharing Bill 2024

The Data Sharing Bill 2024 represents a significant milestone in fostering collaboration and improving data governance within the public sector. By facilitating data sharing between federal government agencies, the Data Sharing Bill 2024 aims to enhance the efficiency and transparency of public service delivery. Passed by the Dewan Rakyat on 12 December 2024, and the Dewan Negara on 19 December 2024, the Data Sharing Bill 2024 focuses on enabling the sharing of data controlled by one public sector agency with another.

A "public sector agency" is defined as (a) the government agency in charge of the public services under Article 132(1) of the Federal Constitution,[1] excluding joint public services and State public services, and (b) statutory authorities vested with powers by federal law. The Data Sharing Bill 2024 proposes, among others, the following:

- **Sharing of data under the control of a public sector agency with other public sector agency**: Public sector agencies may request another public sector agency for the sharing of data under the control of such other public sector agency by specifying the data requested, the purpose for which the data is requested, the public service agencies intended to be the data recipient and the data provider, and the manner in which the data will be handled.

- **Establishment and membership of the National Data Sharing Committee**: A "National Data Sharing Committee" which is responsible to the Cabinet shall be established. The National Data Sharing Committee's responsibilities include among others, formulating policies and strategies related to data sharing, overseeing the effective implementation of the proposed legislation and taking or recommending appropriate steps and administrative actions to resolve difficulties or administrative issues that may arise during the implementation of the proposed legislations.

- **Duties and powers of the Director General of the National Digital Department**: The Director General of the National Digital Department is responsible for, among others, implementing the policies and strategies relating to data sharing formulated by the National Data Sharing Committee, and coordinating and facilitating data sharing under the proposed legislation.

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

Introduction of Online Safety Bill 2024

The Online Safety Bill 2024 marks a significant step in Malaysia's journey toward a safer online environment. Passed by the Dewan Rakyat on 11 December 2024, and subsequently by the Dewan Negara on 16 December 2024, this proposed legislation is designed to regulate harmful content and establish clear duties for applications service providers, content applications service providers and network service providers. The Online Safety Bill 2024 governs (a) any applications service which utilises Internet access service that enables communications between users, (b) any content applications service which utilises Internet access service to provide content, and (c) any network service. However, private messaging feature of any applications service and content applications service are explicitly excluded from its scope. Importantly, the proposed legislation applies both within and outside Malaysia, as outlined in Section 3.

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

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

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

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

- **Duty to implement measures to mitigate risk of exposure to harmful content**: ASPs and CASPs must implement measures specified in the code issued by the MCMC under the proposed Section 80 ("**Code**") to mitigate the risk of users (i.e. users of their services) being exposed to harmful content. They may implement alternative measures, subject to MCMC's approval, if proven to be more effective.

- **Duty to issue guidelines to user**: ASPs and CASPs must issue clear, accessible, and regularly updated guidelines describing the safety measures implemented and terms of use, ensuring they are available to users.

- **Duty to enable user to manage online safety**: ASPs and CASPs are required to make available tools and settings that allow users to manage their safety online, such as preventing unwanted communication and restricting identification.

- **Duty to make available mechanism for reporting harmful content**: ASPs and CASPs must establish a mechanism to enable users to report harmful content available on their services.

- **Duty to make available mechanism for user assistance**: ASPs and CASPs must make available user assistance that is accessible and responsive for users to raise safety concerns, obtain information, and make inquiries.

- **Duty to protect online safety of child user**: ASPs and CASPs must implement measures specified in the Code to ensure safe use of their services by child users, including blocking suspected harmful content from child users, limiting adult-child communication, and regulating personalised content recommendations.

- **Duty to establish mechanism for making priority harmful content inaccessible**: ASPs and CASPs must establish a mechanism to make priority harmful content inaccessible to all users.

- **Duty to prepare Online Safety Plan**: ASPs and CASPs must prepare an Online Safety Plan addressing their compliance with the prescribed duties, ensure it is accessible and regularly updated, and submit a copy to the MCMC.

- **Reporting harmful content**: Users of the services of ASPs or CASPs may report harmful or priority harmful content to ASPs or CASPs, and/or the MCMC. The ASP or CASP (as the case may be) must assess, respond, and take appropriate actions, including dismissing frivolous reports or making content inaccessible.

- **Action by ASPs and CASPs on their own motion**: ASPs and CASPs may also act independently to restrict harmful content if deemed necessary.

- **Enforcement and MCMC oversight**: The MCMC may instruct ASPs and CASPs to make content permanently inaccessible. Non-compliance by the ASP or CASP (as the case may be) with the written instruction issued by the MCMC is in this regard an offence punishable by fine.

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

Amendments to the Penal Code

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

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

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

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

The Communications and Multimedia (Amendment) Bill 2024 was passed by the Dewan Rakyat on 9 December 2024, and subsequently by the Dewan Negara on 16 December 2024. The Communications and Multimedia (Amendment) Bill 2024 proposes pivotal changes to the Communications and Multimedia Act 1998 ("**CMA**"), focusing on enhancing regulatory oversight, broadening enforcement powers, and introducing stricter penalties. Highlights of the proposed amendments to the CMA include:

- **Simplified class licence registration**: A newly proposed Section 46A enables the Minister to dispense with the formalities of registration under a class licence through a Section 13 declaration.[2]

- **Broadening of the MCMC's Powers**: Under the amended Sections 51, 55, and 104, the MCMC is vested with expanded authority to issue directions regarding compliance with the CMA, establish determinations to promote industry conduct that aligns with the objectives of the CMA, and determine mandatory standards including for matters where the MCMC is satisfied that the designated industry forum has not developed a satisfactory voluntary industry code or that the voluntary industry code is likely to fail or has failed, and will continue to fail.

- **Widening of the MCMC's powers to gather information and to conduct audits**: The proposed Section 73A grants the MCMC the authority to conduct audits on licensees whilst the new Section 73B empowers the MCMC to mandate that licensees appoint independent experts for audits at their own expense. The proposed Section 252A introduces obligations for preserving communications data where a police officer or an authorised officer is satisfied that (a) the communications data is reasonably required for an investigation, and (b) there is a risk that the communications data may be destroyed or rendered inaccessible. The proposed Section 252B on the other hand allows a police officer or an authorised officer to issue a written notice requiring the person in control of the communications system to disclose the required communications data where it is deemed reasonably necessary for investigating offences under the CMA or its subsidiary legislation.

- **Network security measures**: The proposed Section 230A allows the MCMC to register certifying agencies for certifying compliance with regulations or standards in relation to network security. Whereas the proposed Section 230B grants the MCMC authority to instruct any person to take the necessary measures to prevent, detect or counter any network security risk.

- **Changes to access agreement registration requirements**: The existing registration requirements under Sections 90 to 93 will be replaced by a lodgement system for access agreements under the amended Section 150. This amendment shifts the responsibility to the parties of the access agreement to ensure compliance with the CMA.

- **Restrictions on harmful content and spam**: The proposed amendments aim to strengthen regulations concerning harmful content and spam. In Sections 211 and 233, the term “offensive” is replaced with “grossly offensive”. Explanations have been added to Section 233 to provide clearer guidelines on the types of content that are prohibited. Section 233 now explicitly covers actions involving fraud or dishonesty against any person. The new Section 233A prohibits the sending of unsolicited commercial electronic messages.

- **Suspension of content applications service**: A new Section 211A empowers the MCMC to suspend services provided by a content applications service provider for non-

compliance with Chapter 2 of Part IX of the CMA or for breaching conditions of its individual or class licence relating to content.

- **Private action for network and fraud damages**: Section 236A introduces a right of private action for damage caused to network facilities or fraud involving access devices.

- **Increased penalties**: Penalties for various offences, including non-compliance with mandatory standards (Section 105), improper network use (Section 233), and unlicensed operations (Sections 126 and 206), have been increased.

The Communications and Multimedia (Amendment) Bill 2024 will now be presented for Royal Assent. Once gazetted, it will become law, taking effect on a date determined by the Minister of Communications.

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

Introduction of Malaysian Media Council Bill 2024

The Malaysian Media Council Bill 2024, which aims to establish the Malaysian Media Council, was tabled for its first reading at the Dewan Rakyat on 12 December 2024. The proposed legislation seeks to empower the Malaysian Media Council to set standards and establish a code of conduct for media practitioner and independent media practitioner in accordance with the standards of ethical and responsible journalism. However, there has been no development since the first reading of the proposed legislation.

Amendments to the Personal Data Protection Act 2010

In our July 2024 Legal Update, we discussed the significant changes introduced by the Personal Data Protection (Amendment) Bill 2024, which was passed by the Dewan Rakyat on 16 July 2024. The proposed legislative amendments, which aim to amend the Personal Data Protection Act 2010, were subsequently passed by the Dewan Negara on 31 July 2024, and have since been gazetted as the Personal Data Protection (Amendment) Act 2024 ("**PDP Amendment Act**"). The provisions of the PDP Amendment Act will come into force in three phases:

- 1 January 2025: Sections 7, 11, 13 and 14 of the PDP Amendment Act will take effect;

- 1 April 2025: Sections 2, 3, 4, 5, 8, 10 and 12 of the PDP Amendment Act will take effect; and

- 1 June 2025: Sections 6 and 9 of the PDP Amendment Act will take effect.

For recapitulation, the points discussed in our July 2024 Legal Update are summarised as follows:

- The term “data user” will be replaced with “data controller”, aligning with global data protection terminology. However, the existing definition for “data user” remains unchanged.

- The penalties for non-compliance with any of the Personal Data Protection Principles will be significantly increased, with fines raised from RM300,000 to RM1,000,000 and/or imprisonment extended from a maximum term of 2 years to a maximum term of 3 years.

- Previously applicable only to data controllers, the Security Principle will directly bind data processors.

- Data controllers must notify the Personal Data Protection Commissioner (“**Commissioner**”) of any personal data breaches as soon as practicable. Failure to do so could result in a fine of up to RM250,000 and/or imprisonment for up to 2 years. The relevant data subject must also be notified where the personal data breach causes or is likely to cause any significant harm to the data subject.

- Both data controllers and data processors must appoint data protection officer(s), who shall be accountable to the data controller or data processor.

- Rights to data portability will be introduced in favour of the data subjects, subject to technical feasibility and compatibility of the data format.

- In terms of cross-border transfer of personal data, the pre-existing “whitelist” approach will be abolished. Data controllers will be able to transfer personal data out of Malaysia so long as the prescribed conditions are met.

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

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

On 18 November 2024, the Commissioner and Futurise Sdn. Bhd. issued a joint press release providing updates on Malaysia’s Personal Data Protection and Privacy Regulatory Sandbox. As part of the sandbox's deliverables, 4 guidelines and 1 standard will be released by early 2025, while 3 further guidelines will be released in the third quarter of 2025. These guidelines are set to provide clear, actionable frameworks for the private sectors to ensure compliance with evolving data protection regulations and international standards.

Introduction of Cyber Security Act 2024

We have discussed the Cyber Security Act 2024 in our April 2024 and August 2024 Legal Updates.

Our April 2024 Legal Update focused on the key provisions of the Cyber Security Act 2024 applicable to national critical information infrastructure entities and cyber security service providers, including the implementation of the measures, standards and processes specified in the code of practice, notification of cyber security incidents, the conduct of cyber security risk assessments and audits, the licensing of cyber security service providers.

Our August 2024 Legal Update discussed the 4 pieces of subsidiary regulations introduced under the Cyber Security Act 2024, namely:

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

Since then, the Chief Executive of the National Cyber Security Agency has issued the following directives pursuant to his statutory powers under Section 13 of the Cyber Security Act 2024:

- Directive No. 1: Notification of Cyber Security Incident;
- Directive No. 2: Licensing of Cyber Security Service Provider;
- Directive No. 3: Designation of National Critical Information Infrastructure Entity;
- Directive No. 4: National Cyber Security Baseline Self-Assessment; and
- Directive No. 5: Cyber Security Risk Assessment.

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

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

We discussed the Communications and Multimedia (Licensing) (Amendment) (No. 2) Regulations 2024 and Communications and Multimedia (Licensing) (Exemption) (Amendment) Order 2024 in our October 2024 Legal Update.

As a refresher, starting from 1 January 2025, providers of Internet messaging services and social media services with 8 million or more users in Malaysia will be required to obtain an applications service provider class licence under the CMA to offer their services within Malaysia.

Following a public consultation and the eventual release of the Public Consultation Report on the *draft Code of Conduct (Best Practice) for Internet Messaging Service Providers and Social Media Service Providers* on18 December 2024, the MCMC has on 20 December 2024 published the *Code of Conduct (Best Practice) for Internet Messaging Service Providers and Social Media Service Providers*, which sets out the best practice for adoption by Internet messaging service providers and social media service providers licensed under the CMA in addressing harmful content online, as well as other relevant conduct requirements. The Code of Conduct aims to ensure that service providers uphold online safety and security, particularly for children and vulnerable groups.

Introduction of The National Guidelines on AI Governance & Ethics

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

The objectives of the AI Guidelines are as follows:

- supporting the implementation of the Malaysian National AI Roadmap 2021-2025;
- facilitating the implementation of responsible AI according to the 7 AI Principles;
- building trustworthiness in AI, which is emphasised by responsible AI;
- managing risks caused by the development and deployment of AI technology; and
- maximising the benefits of AI to enhance national productivity, economic growth and competitiveness.

Concluding Remarks

The TMT legal advancements of 2024 underscore Malaysia's proactive approach in addressing the challenges and opportunities of the digital era. These reforms not only enhance the regulatory framework but also pave the way for sustainable growth, innovation, and greater trust in the ICT sector and beyond. As stakeholders navigate this evolving landscape, the focus must remain on ensuring that these laws are effectively implemented and continue to serve the interests of a rapidly transforming society.

For further enquiries, please contact:

Janet Toh Yoong San
Co-Head, Technology, Media & Telco
Head, Personal Data Protection & Privacy
E: janet.toh@shearndelamore.com
P: +603 2027 2978

Boo Cheng Xuan
Associate, Technology, Media & Telco
Associate, Personal Data Protection & Privacy
E: boo.chengxuan@shearndelamore.com
P: +603 2027 2662

Yee Yong Xuan
Associate, Technology, Media & Telco
Associate, Personal Data Protection & Privacy
E: yongxuan.yee@shearndelamore.com
P: +603 2027 2615

This Legal Update is written by the abovementioned lawyers with the assistance of our pupil-in-chambers, **Muhammad Sirhan Sidqi Bin Abdul Aziz**.

[1] Article 132(1) of the Federal Constitution provides that for the purposes of the Federal Constitution, the public services are: (a) the armed forces; (b) the judicial and legal service; (c) the general public service of the Federation; (d) the police force; (e) *(Repealed)*; (f) the joint public services mentioned in Article 133; (g) the public service of each State; and (h) the education service.

[2] Section 13(1) of the CMA provides that the Minister may, from time to time, make a written declaration that an individual licence, or a class of individual licences, or a class licence: (a) is subject to such conditions; or (b) enjoys such benefits, as the Minister deems fit.