ASL
Adnan Sundra & Low

KEY LEGISLATIVE UPDATES IN MALAYSIA'S CYBER SECURITY, MEDIA AND TECHNOLOGY SECTORS

MONTH :
January 2025

BY :
Sri Sarguna Raj,
Steven Cheok Hou Cher
& Nicole Chong

Key Legislative Updates in Malaysia's Cyber Security, Media and Technology Sectors

Recent legislative developments have marked significant changes across the legal landscape in Malaysia, notably a series of transformative reforms within the cyber security, media and technology sectors. Below is a key overview of these laws/guidelines and their implications, with references to specific provisions and sections where applicable.

1. Communications and Multimedia Act ("CMA") (Amendment) Bill 2024

Status: Passed on 16 December 2024. To be gazetted and take effect on a specified date.

Overview: The Communications and Multimedia Act (Amendment) Bill 2024 ("**CMA Bill**") introduces stringent measures to enhance regulatory oversight by the Malaysian Communications and Multimedia Commission ("**MCMC**"). Key updates include a class licensing framework for social media as well as enhanced penalties for online offences.

Implications:

- **Dispense with Formalities:** The new insertion of section 46A grants the Minister of Communications discretionary powers to declare, under section 13, any person operating under a class licence to be registered without the need for formalities of registration for that class licence.
- **Licensing Requirement:** Pursuant to the Communications and Multimedia (Licensing) (Exemption) Order 2000 and the Communications and Multimedia (Licensing) Regulations 2000, Application Service Providers ("ASP") offering social media platforms and messaging services must now obtain the Applications Services Provider Class (ASP(C)) licence by 1 January 2025 under the CMA. This shall apply to ASPs with at least 8 million registered users in Malaysia, including cloud service providers, internet access service providers and public cellular services.

- **Suspension of Services in relation to Content:**

  The new insertion of **section 211A** allows the MCMC to direct a content applications service provider to suspend its services for a specified period in light of any contravention to content requirements (Chapter 2 of Part IX of the CMA), any breach of licensing conditions in relation to content, or any non-compliance with any instrument from the Minister of Communications or the MCMC in relation to content.

- **Stronger Enforcement: Section 233**, which seeks to govern acts relating to the improper use of network facilities or services, has now been expanded to cover "grossly offensive" communications (previously only "offensive") as well as contents involving "fraud or dishonesty against any persons". There are not only increased penalties under Section 233, but there are also enhanced penalties of up to five years' imprisonment that apply for offences targeting minors.

- **Heftier Punishments:**

  (a) Non-compliance with the direction of the MCMC (Section 53): The punishment for non-compliance with MCMC's direction(s) under section 53 has been increased from RM300,000 or imprisonment not exceeding 3 years or both to RM1,000,000 or imprisonment term not exceeding 10 years or both. The offender shall also be liable to a fine of RM100,000 for every day or part of a day during which the offence is continued after the conviction.

  (b) Penalty (Section 242): Where there are omissions to comply with the CMA, breach of licence conditions or when dealing with offences where there is no specific penalty provided under the CMA, the penalties imposed have been increased from a fine of up to RM100,000 and/or imprisonment for up to 2 years to a fine of up to RM1,000,000 and/or imprisonment for up to 5 years.

- **Audit requirements (Sections 73A and 73B):** The addition of sections 73A and 73B grants the MCMC powers to conduct audits or order that an independent audit be

conducted at the licensee's own expense. This discretionary power granted to the MCMC was previously not observed under the CMA. Notably, anyone who fails to comply with these provisions commits an offence.

2. Online Safety Bill 2024

Status: Passed on 16 December 2024. To be gazetted and take effect on a specified date.

Overview: The Online Safety Bill ("**OSB**") aims to protect individuals, especially vulnerable groups such as children, from online harms such as cyberbullying, exploitation, and misinformation. Key measures are detailed in **sections 13-19**.

Applicability: Applies to service providers licensed under the CMA, i.e. licensed network service providers, application service providers and content applications service providers.

Implications:

- **Focus Areas:** The OSB, in general, regulates contents concerning "harmful content" (First Schedule) and "priority harmful content" (Second Schedule). In terms of the Second Schedule, it covers a more stringent regulation with regards to: (1) Content on child sexual abuse material as provided for under section 4 of the Sexual Offences against Children Act 2017; and (2) Content on financial fraud.
- **Platform Responsibilities towards the Protection of Users:**
  - **(a)** **Section 13** imposes a duty whereby the licensed service providers must implement measures to detect and mitigate harmful content.
  - **(b)** **Section 16** provides that platforms must implement robust reporting mechanisms, such as easily accessible complaint channels for users.
  - **(c)** **Section 18** specifically provides for the duty of service providers to ensure the protection of child users relating to online safety.
  - **(d)** **Section 19** states that there should be a mechanism in place to make priority harmful content inaccessible to all users.

3. Data Sharing Bill 2024

Status: Passed on 19 December 2024. To be gazetted and take effect on a specified date.

Overview: The Data Sharing Bill ("**DSB**") establishes a structured framework for data sharing between public sector agencies and introduces the National Data Sharing Committee ("**NDSC**"), detailed in **sections 5-10**. It also outlines the duties and powers of the Director General of the National Digital Department. This law's impact modernizes public sector operations whereby the DSB seeks to streamline data sharing among public agencies. Doing so would improve service delivery, whereby there will be faster processing of welfare applications and real-time updates on public health data.

Applicability: Public sector agencies and organizations involved in handling and sharing sensitive data.

Implications:

- **Centralized Oversight:** The DSB introduces the NDSC, which will formulate policies and strategies in relation to data sharing, oversee the effective implementation of the DSB and to take appropriate steps to resolve the issues arising when implementing the DSB. It also outlines the duties and powers of the Director-General of the National Digital Department.
- **Improved Efficiency:** Introduces streamlined data exchange processes aimed to enhance government service delivery and complement the Public Sector Data Sharing Policy. This includes provisions on:
  (a) Circumstances where the public sector agencies may request data from other agencies
  (b) Conditions in relation to the sharing of data, such as the purpose for which data may be shared, as well as the duties of the data providers and data recipients.

4. Penal Code (Amendment) (No.2) Bill 2024 and Criminal Procedure Code (Amendment) (No.2) Bill 2024

Status: Passed on 10 December 2024. To be gazetted and take effect on a specified date.

Overview: The amendments aimed to fill gaps in potential cyberspace offences, introducing specific provisions addressing online bullying.

Applicability: The law applies to individuals and entities engaging in or facilitating bullying behaviour.

Implications:

- **New and Specific Offences:** Addresses that bullying is becoming a concern and introduces bullying-related offences:
  (a) offences causing harassment, distress, fear or alarm (**Section 507B**);
  (b) offences causing harassment, distress, fear or alarm to a person likely to feel harassed, distress, fear or alarmed (**Section 507C**);
  (c) offences causing a person to believe that harm will be caused (**Section 507D**),
  (d) offences of publishing identity information, causing harassment, distress, fear or alarm (**Section 507E**); and
  (e) offences of publishing identity information causing a person to believe that harm will be caused (**Section 507F**)
- **Stricter Penalties:** Enhanced legal repercussions aim to deter such behaviour, including online and offline bullying.

5. Malaysian Media Council Bill 2024

Status: Passed the first reading on 12 December 2024, expected to be tabled for second reading in February 2025.

Overview: The Malaysian Media Council Bill 2024 ("**MMC Bill**") proposes the establishment of the Malaysian Media Council ("**MMC**") as a self-regulatory body to uphold journalistic standards and resolve media disputes, as outlined in **sections 3-15**.

Applicability: Media organizations, journalists, and stakeholders in the media industry.

Implications:

- **Self-Regulation:** The MMC Bill sets up a self-regulating body known as the MMC to safeguard the interests of the media and media practitioners. **Section 8** provides that the composition of the MMC will consist members from the media companies (publisher or senior management, media associations (members, media practitioners and independent media practitioners and non-media members, e.g. academicians, NGOs and the public.
- **Reporting Mechanism: Section 15** allows the MMC to develop a complaints and dispute resolution mechanism which serves to oversee media practices and addresses public complaints.
- **Professional Standards:** A professional code of conduct will be established by the MMC for media practitioners. A database of media practitioners shall be established, managed and maintained for data collection purposes and statistics.
- **Binding Powers: Section 21** empowers MMC to issue binding guidelines, directives, circulars, standards and notices to all members.
- **Disciplinary Action: Section 16** allows MMC to take disciplinary action against members who have committed a misconduct pursuant to the code of conduct, circular, guideline or instruction or those who have breached the binding regulations issued under section 21.
- **Potential Replacement:** The MMC Bill hopes to answer the calls to repeal the Printing Presses and Publications Act 1984.

6. Cyber Security Act 2024

Status: Effective on 26 August 2024.

Overview: There was previously no unified law regulating cyberspace in Malaysia. Through the enactment of the Cyber Security Act ("CSA"), the CSA has marked a key milestone in strengthening Malaysia's cyber defences. This includes the establishment of the National Cyber Security Committee and the licensing requirement for cybersecurity service providers.

Applicability: In relation to licensing, this would apply to organizations offering cybersecurity services.

Implications:

- Mandatory Licensing (Section 27): From 1 January 2025 onwards, a service provider who provides or intends to provide any cybersecurity service or advertise itself as a cyber security service provider is required to apply for a cybersecurity service provider license under the CSA. The applicable services are provided under the Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024, namely:

  (i) Managed security operation centre monitoring services - The monitoring of cyber security levels to identify or detect cyber security threats, or the determining the necessary measures to respond to or recover from any cyber security incidents, and preventing such incidents from occurring in the future; and/or

  (ii) Penetration Testing services - Assessing, testing, or evaluating the level of cyber security, including:

  a. Determining cyber security vulnerabilities and demonstrating how these vulnerabilities may be exploited;

  b. Determining or testing the organization's ability to identify and respond to cyber security incidents through simulated attempts to penetrate its cyber security defences;

  c. Identifying and measuring cyber security vulnerabilities, preparing appropriate mitigation procedures to eliminate or reduce these vulnerabilities to an acceptable level of risk; or

  d. Utilizing social engineering methods to assess the level of vulnerability of an organization to cyber security threats.

  The licensing obligations do not apply to:

a) government entities; or

b) persons, other than a company, to its related company; or

c) where the computer or computer systems are located outside Malaysia.

- Subsidiary Legislations and Directives issued to complement the CSA:

  <u>Subsidiary Legislations</u>

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

  <u>Directives</u>

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

- **Severe Penalties (Section 20):** Non-compliance with the licensing requirements under the CSA is severe, whereby upon conviction, the person shall be liable to a fine up to RM500,000, imprisonment for a term not exceeding 10 years, or both.

Once the approval process has been completed, NACSA will provide a list of licensed cyber security service providers on its licensing portal. To ensure compliance, companies should verify their licensing statuses or their cyber security service provider's licensing statuses.

7. The National Guidelines on AI Governance & Ethics

Status: Launched on 20 September 2024.

Overview: The government recognises the robust development in Artificial Intelligence ("**AI**") and introduced the National Guidelines on AI Governance & Ethics ("**The National Guidelines**"). The National Guidelines provide a comprehensive framework for the responsible development and deployment of AI in Malaysia. Sections 1 and 2 provide a general introduction to the knowledge and application of AI. Section 3 details the different roles and responsibilities of the key stakeholders through the following:

Applicability: The guidelines are applicable to users, developers, businesses, and public sector agencies involved in the use or creation of AI technologies across various industries.

Part A: The National Guidelines for AI End Users

- Targets individuals and organizations using AI products and services such as virtual assistants, healthcare tools, and fraud detection systems.
- Encourages awareness about responsible AI use, empowering users to understand their rights, responsibilities, and the implications of AI adoption.
- Focuses on promoting transparency and informed decision-making for ethical AI.

Part B: The National Guidelines for Policy Makers in Government, Agencies, Organizations and Institutions

- Targets government officials, agencies, and organizations responsible for creating and implementing AI-related policies.
- Outlines a framework to ensure ethical AI deployment, emphasizing compliance, consumer protection, and fair competition.
- Encourages international collaboration and the development of standards for trustworthy AI systems, balancing innovation with societal values.

C. The National Guidelines for Developers, Designers, Technology Providers and Suppliers

- Directed at professionals designing and deploying AI systems, including developers, engineers, and researchers.
- Provides best practices and technical standards to align AI

development with ethical principles, mitigating risks such as bias or data misuse.

- Encourages continuous evaluation and refinement to ensure AI aligns with human values, legal standards, and sustainability goals.

Conclusion

The legislative updates of 2024 represent Malaysia's commitment to strengthening digital governance, enhancing user safety, and fostering accountability in cyber security, media and technology sectors. Businesses and stakeholders must stay informed and compliant to navigate these transformative changes effectively.

This article was written by our partners, Sri Sarguna Raj, Steven Cheok Hou Cher & Nicole Chong from the Intellectual Property, Media, Sports & Gaming Practice Group, with the assistance of Soo An Qi, Lim Chaw Zen and Michelle Yap Siew Hui (Senior Associate, Associate & Pupil). It contains general information only. It does not constitute legal advice or an expression of legal opinion and should not be relied upon as such.