Key Updates to the Communications and Multimedia (Amendment) Act 2025 and Recommendations for Industry Preparedness

Introduction

The Communications and Multimedia (Amendment) Act 2025 ("**Amendment Act**") came into operation on 11 February 2025 except for **section 92** (prohibition of sending of unsolicited commercial electronic messages) and **section 112** (preservation and disclosure of communications data by police or unauthorised officer) of the Amendment Act.

Key Amendments Introduced in the Amendment Act

The amendments to the Communications and Multimedia Act 1998 ("**CMA**"), primarily aimed at addressing network security risks and enhancing MCMC's enforcement powers.

Below are the key amendments, which are generally divided into three categories – Industry Development, Network Security Risks and Expansion of MCMC's Power and our recommendations on how we believe the industry players should be prepared.

Industry Development		
Amendments	**Explanation**	**Recommendations**
Simplified Processes for Access Agreements to Provide Flexibility for Industry Players	• **Section 150** is amended to simplify the process for access agreements by requiring them to be lodged with MCMC, eliminating the previous complex review and registration process under Sections 90 to 93 of the CMA (repealed).	• Establish an internal workflow to ensure timely lodging of access agreements with MCMC.
Duty to Protect Consumers' Interests Applies to All Service Providers	• **Section 188(1)** is amended to apply to all service providers, compelling them to deal reasonably with consumers and effectively handle all consumer complaints, with no exceptions. This change is made by deleting Section 187, which allows exceptions for non-individual or non-class licence holders. • **Section 188(2)** is amended to empower MCMC to issue directions to service providers to comply with Subsection (1), and failure to comply with these directions will result in a penalty of up to RM1 million, as specified in the new **Subsection (3)**.	• Implement a robust customer complaint management system that records and tracks all complaints. • Develop standard operating procedures (SOPs) to handle complaints efficiently and effectively. • Regularly review complaint handling processes to ensure compliance with MCMC guidelines. • Provide comprehensive training to customer-facing staff to enhance their ability to handle complaints in a compliant manner.
Rights of Private Action	• **Section 236A** (new provision) grants the right of private action to any	• Conduct a risk assessment to identify potential

	person to seek relief in civil proceedings against alleged offenders, regardless of whether they have been charged with an offence under the CMA. This applies to any persons who have suffered losses due to violations of Sections 235 (damage to network facilities) and 236 (fraud-related activities involving access devices).	vulnerabilities that could lead to civil claims. • Implement preventive measures such as enhanced network security protocols to minimize risks. • Develop a crisis management plan to address potential claims promptly and effectively.
Increased Penalties	• The Amendment Act generally increases the maximum fine to RM1 million and the maximum imprisonment to ten years for most offences under the CMA. • Whereas the previous maximum fines under the CMA were in the hundreds of thousands, with imprisonment ranging for a few months to five years.	• Perform a comprehensive compliance audit to identify any gaps in adherence to the CMA. • Develop a corrective action plan to address any areas of non-compliance. • Enhance internal policies and procedures to reflect the heightened penalties and ensure compliance. • Conduct regular compliance training for all employees to raise awareness of the new penalties and the importance of adhering to regulations.
Network Security Risks		
Powers to Address Network Security Risks	• **Section 230B** (new provision) provides the MCMC with the power to instruct any persons to take specific measures or comply with specific requirements to prevent, detect, or counter a network security risk. A "network security risk" is defined as "*any risk or threat, if exploited or not mitigated, could pose a significant risk of damage or disruption to the operation of network facilities, network services, or application services*".	• Conduct regular network security assessments to identify potential risks and vulnerabilities. • Develop and implement a comprehensive cybersecurity policy to address identified risks. • Create an incident response team to handle network security issues swiftly and efficiently. • Stay updated on MCMC's security directives and ensure prompt compliance with any issued instructions.
Amendments to Section 233 of the CMA – Addressing Prohibited Content	• **Section 233(1)(a)** is amended, replacing the term '*offensive'* with '*grossly offensive'*. The Section has also been expanded to include transmitting prohibited content with the intent to commit offences involving '*fraud or dishonesty against any person*' as new offence.	• Review and update internal content policies to ensure alignment with the updated definitions of prohibited content. • Implement automated monitoring tools to detect

	• The Amendment Act introduces Explanations 1 to 6 under Section 233 (previously absent), specifying the types of prohibited content, such as indecent, obscene, false, menacing or grossly offensive material. • **Section 233(2)** (previously under Subsection (3)) is amended to impose a higher penalty for offences under Subsection (1), with a fine of up to RM500,000 (previously RM50,000) and/or imprisonment for up to two years (previously one year), with further fines of RM5,000 (previously RM1,000) per day the offence continues after conviction. • **Section 233(3)** (new provision) is inserted to address offences under Subsection (1) committed against a minor, where the offender may be subject to imprisonment for up to five years. • The previous Section 233(2) becomes **Section 233(4)**. • **Section 233(5)** is introduced to impose penalties for offences under Subsection (4), with a fine of up to RM1 million and/or imprisonment for up to five years, with further fines of RM10,000 per day the offence continues after conviction.	and remove prohibited content promptly. • Establish a clear escalation process for handling detected prohibited content, particularly content involving minors. • Provide clear guidance and training to content moderators to help them identify and manage prohibited content effectively.
Specific Provision on Spam	• **Section 233A** (new provision) specifically prohibits the sending or causing / authorising the sending of "*unsolicited commercial electronic messages*" (i.e., spam). • Previously, under the CMA, offences related to spam are typically addressed under the general provision of Section 233(1)(b).	• Audit all marketing and communication practices to ensure compliance with spam regulations. • Implement systems to obtain and record user consent for marketing communications. • Establish a clear opt-out mechanism for users to easily withdraw their consent. • Train marketing teams on the importance of respecting user preferences and adhering to spam regulations.

Expansion of MCMC's Power		
MCMC Empowered to Suspend the Services of the Content Application Service Providers	• **Section 211A** (new provision) provides the MCMC with the power to direct the content application service providers to suspend their services if they are in violation of the CMA and its prescribed obligations thereunder.	• Develop a compliance framework to prevent service violations. • Regularly review service offerings and terms of use to ensure they comply with the CMA. • Establish a monitoring system to detect potential violations early. • Engage with MCMC proactively to address any compliance concerns before they escalate.
MCMC Empowered to Conduct Audits	• **Section 73A** (new provision) provides the MCMC with the ability to conduct audits on any licensee or service providers relating to communications systems on any matter under the CMA, its subsidiary legislation, any instrument issued under the CMA, or any information furnished to the MCMC. • **Section 73B** (new provision) allows the MCMC to require any licensee to appoint its own independent expert to carry out an audit, with the licensee bearing the costs of the appointment.	• Maintain detailed and accurate records of all compliance-related activities. • Conduct internal audits regularly to identify and address potential compliance issues. • Identify and engage independent auditors in advance to be prepared for MCMC's audit requirements. • Allocate resources and budget for potential audit costs to avoid unexpected financial strain. • Ensure audit findings are documented and addressed promptly.

Conclusion

The introduction of the Amendment Act calls for affected parties to thoroughly examine the changes to ensure compliance with the evolving regulatory framework, especially considering the heightened penalties for certain offences. In particular, with the expanded enforcement powers addressing prohibited content, content application service providers are advised to take proactive measures in monitoring and removing infringing material to minimise the risk of service suspension. Licensees should also exercise greater diligence in adhering to the provisions of the CMA and their licence conditions, in light of the stricter penalties set out in the Amendment Act.

Should you have any questions or concerns, please do not hesitate to contact:



Ariff Firman Bin Mohd Sidek
Partner
White-Collar Crime and Corporate Investigations
arifffirman@law-partnership.com



Nur Aliya Syaffa Binti Johari
Associate
White-Collar Crime and Corporate Investigations / Corporate and Commercial
aliyajohari@law-partnership.com

©LAW Partnership 2025. All rights reserved.