



# Malaysia's Licensing Regime: Enhancing online safety and digital market accountability

December 2024

# Overview of the New Regulatory Framework (Preamble)

On **1 August 2024**, the **Malaysian Communications and Multimedia Commission (MCMC)** gazetted a **new regulatory framework** for **social media services** and **internet messaging service providers (Service Providers)**. This framework represents a landmark shift in Malaysia's digital regulation landscape, aligning with global regulatory trends, such as the EU's Digital Services Act<sup>1</sup> (DSA) and the Digital Markets Act<sup>2</sup> (DMA), which seek to enhance platform accountability and user protection. The introduction of this framework signals Malaysia's commitment to ensuring consumer protection, while addressing content regulation challenges, such as misinformation, cyberbullying, scams, and harmful or illegal material.

Prior to the introduction of this regulatory framework, Service Providers were **exempted** from obtaining a license pursuant to the Communications and Multimedia (Licensing) (Exemption) Order 2000.

However, under the new regulations, any Service Provider with **at least 8 million users in Malaysia** must obtain an **Applications Service Provider Class (ASP(C)) License** from the MCMC. Social media and messaging platforms, including **Facebook, Instagram, TikTok, WhatsApp, and Telegram**, are expected to comply with this framework within the **five-month grace period** from 1 August 2024. Providers failing to secure the ASP(C) License by 31 December 2024 may face penalties and enforcement actions.



1. DSA applies to providers of intermediary services offered to users based in the EU, regardless of where the providers themselves are established.
2. DMA applies to large digital platforms in the EU that intermediate between businesses and users. It establishes new rules to ensure fair and open digital markets and enable more business and user choices on how they use digital services.



# Key issues driving Malaysia's push for digital oversight

Online harm is a significant concern in Malaysia, with issues such as graphic violence, child exploitation, online scams, and gambling, bullying and harassment, and cyberbullying affecting many users.<sup>3</sup>

The Malaysian government's efforts to regulate such Service Providers are part of a broader global trend to address online harm, and ensuring online safety. Other countries in the APAC region, such as Singapore, Indonesia, Thailand, and India have also implemented regulations to address similar issues. The Malaysian government's approach to regulating Service Providers is likely to involve a combination of measures, including licensing requirements, content moderation, and user reporting mechanisms.



## Why does this matter?

This regulatory framework supports the country's digital transformation initiatives by promoting a secure and well-regulated digital ecosystem. It establishes guidelines that enhance trust and safety for users, particularly safeguarding against online harms, such as scams, cyberbullying, and misinformation. At the same time, it ensures that data privacy and security measures are upheld. By regulating major platforms, the framework seeks to create a safer and more accountable online environment for all users.

3. Statistics on Online Harm in Malaysia highlighted: (a) 100,000 children at risk of online sexual exploitation and manipulation; (b) 42,000 reports of online gambling-related suspicious transactions; (c) 28% of Malaysian children have been victims of online violence or cyberbullying; (d) 9,483 reports of cyberbullying received by MCMC from January 2022 to July 2024; (e) RM 1.4 billion in losses due to scams



# Key obligations of the Regulatory Framework

1

## Licensing requirement:

Platforms with a substantial Malaysian user base must apply for an **ASP(C) License**. The application must be submitted by **31 December 2024**.

2

## Local Incorporation:

Service providers must be **locally incorporated** in Malaysia to meet the licensing requirements, which may present challenges for foreign-based companies.

3

## Content moderation and safety:

Platforms are required to implement **robust content moderation measures** to address harmful content such as misinformation, cyberbullying, and **illegal material**. This includes having processes to handle user complaints and ensure prompt removal of flagged content.

4

## Reporting obligations:

Platforms must submit regular reports to the MCMC, detailing their compliance with content moderation and safety protocols.



# Licensee's obligations

Once the relevant Service Providers are licensed by the MCMC, they will be required to fulfil certain obligations under the **Communications and Multimedia Act (CMA), its subsidiary legislation(s). They must also adhere to any licensing conditions imposed by the MCMC, the Content Forum's Content Code, General Consumer Code, and relevant principles and provisions under the Personal Data Protection Act 2010.**

To supplement the new regulatory framework, the MCMC recently issued a Draft Code of Conduct (Best Practices) for Internet Messaging Service Providers and Social Media Service Providers. Public consultation on the draft code concluded on 5 November 2024, with final guidelines anticipated to be published by 1 January 2025.

The draft outlines best practices for licensed Service Providers to tackle harmful online content, structured around four key pillars:



User safety



Child safety measures



Risk mitigation



Accountability

In implementing these pillars, licensed Service Providers will be guided by conduct obligations.

These pillars aim to ensure that platforms adopt robust content moderations practices, including timely removal of harmful material and safeguarding users – especially minors – from online risks. Specific obligations include implementing age verification measures, maintaining transparency in handling user reports, and conducting regular risk assessments to identify and mitigate systemic risks. Licensed Service Providers will also be required to submit periodic reports on compliance efforts.



# How do Malaysia's rules compare to the EU's Digital Services Act package?



## EU Requirements Overview

The Digital Services Act (DSA) and the Digital Markets Act (DMA) are two significant pieces of legislation introduced as part of the EU's drive to ensure "A Europe fit for the Digital Age" along side other regulatory requirements such as the EU's AI Act and Data Act among others.

The DSA entered into force for the largest companies in August 2023, while all other relevant companies became subject to its requirements February 2024. The DMA came into effect in March 2024. The DSA creates wide-ranging requirements for product design, risk management, corporate governance, public reporting, dispute resolution, and researcher access to data – as well as a mandatory independent audit of compliance. It aims to hold internet companies accountable for making the internet safer and more trustworthy. While the DMA is largely focused on competition and aims to address the perceived 'unfair practices' of the very biggest digital platforms which have been classified as 'gatekeepers'.







## Key provisions of the Digital Markets Act

The DMA targets the 'gatekeepers' that occupy dominant roles in core platform services and have strong economic and intermediation positions in digital markets. While it applies to a broad range of archetypes, including operating systems, messaging, web-browsers and virtual assistants etc. the thresholds for being designated a gatekeeper are very high.

In-scope companies are required to notify the European Commission (EC) when they reach certain quantitative thresholds which act as a precursor to gatekeeper status. These include:



EU revenue of at least €7.5 billion in each of the last three financial years or an average market capitalization of at least €75 billion in the last financial year, while providing the same core platform service in at least three EU Member States' and



At least 45m monthly active users in the EU, and at least 10,000 yearly active EU business users in the last three financial years.

However, to fall under the DMA's scope, a company must also meet qualitative thresholds including an entrenched and durable position; have significant impact on the EU market; and control an important gateway for business users towards consumers. Further, entities meeting the quantitative thresholds have the opportunity present arguments as to why they should not be classified as gatekeepers.

Currently, there are seven companies designated as gatekeepers under the DMA – Apple, Amazon, Alphabet, Booking, Meta, ByteDance and Microsoft with 24 of the 'core platform services' provided by these companies in scope of the requirements.

The DMA requires designated gatekeepers to adhere to specific rules designed to prevent unfair practices within their platforms. Obligations include:

- Ensuring customers have the ability to switch between platforms easily without restrictions;
- Requiring users' consent for use of personal data for advertising or across products;
- Reporting on certain data uses and ensuring users' free access to data;
- Restricting use of businesses' data to develop competing products or services and ensuring businesses have access to the data they generate on the platform;
- Ensuring that services and products offered by the gatekeeper are ranked impartially i.e. no preferential treatment over those of third parties offered on their platform;



## Key provisions of the Digital Services Act

The DSA imposes transformative obligations that turn many operational domains into heavily regulated business activity, including product development, content moderation, and content recommendation. The requirements include tiered cumulative obligations for intermediary services, hosting services and online platforms with the most onerous requirements applied to those designated as very large online platforms (VLOPs) or very large search engines (VLSEs). VLOPs and VLSEs are designated on the basis of having 45 million or more monthly active users in the EU and to date the EC has designated 24 VLOPs / VLSE under the DSA. Obligations include:

- Content moderation including user-friendly notice and takedown mechanisms, complaint-handling systems, redress mechanisms for users, and preferential response to notices from trusted flaggers;
- Requirements to implement safeguards to protect children's rights;
- Transparency reports on content removal including a requirement to publish reports explaining and justifying the decision process;
- Requirement to develop and maintain a public ad repository which includes information on the ads shown on the platform for the past 12 months;
- Requirement to inform users on why they are seeing an ad, who the ad is for and ad targeting information;
- Requirements relating to recommender systems transparency such as including the main parameters for recommendations in the terms and conditions, users should also be able to choose not to receive recommendations based on profiling;
- Mandatory risk assessments and adoption of appropriate mitigation measures to address systemic risks, including illegal content and human rights violations;
- Requirements to conduct an independent audit annually and appoint a compliance function with sufficient authority and resourcing to perform significant duties including monitoring compliance, informant and advising management and staff about compliance, and ensuring all systemic risks are managed.





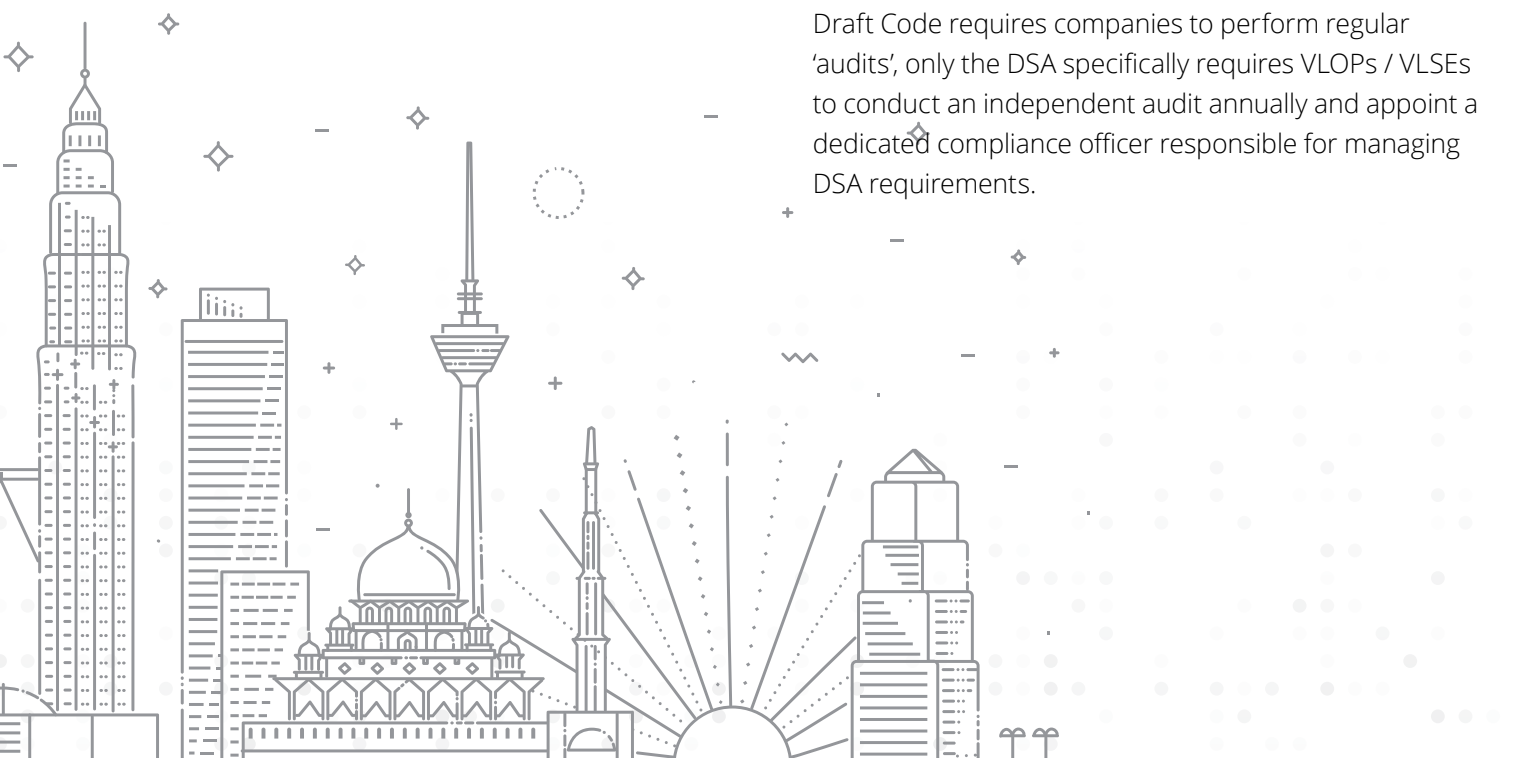
# How does this compare with Malaysia's New Rules?

The number of companies that fall within scope of the new regulatory framework in Malaysia is very small whereas a much larger number of companies are required to comply with the DSA. That being said, both the DMA and the most onerous requirements of the DSA are only applicable to a select few very large companies that meet specific criteria and have been designated 'gatekeepers' and VLOPS / VLSEs, respectively.

Malaysia's framework primarily focuses on content management with the aim of promoting user safety, mitigating and managing risks, and ensuring accountability of digital platforms. In contrast, the DSA creates wide-ranging requirements for product design, risk management, corporate governance, public

reporting, dispute resolution, and researcher access to data. Whereas the DMA specifically seeks to address anti-competitive behavior by large 'gatekeepers' – something not directly addressed in either Malaysia's licensing requirements or its Draft Code of Conduct.

Malaysia's approach to content management is also narrower, with the targeted goal of enhancing child safety and addressing harmful online behaviour. It applies exclusively to social media and messaging platforms. Conversely, the DSA targets a wider range of digital service providers including e-commerce platforms, online marketplaces, and hosting platforms. It also focuses on a broader set of systemic risks, has more requirements relating to targeted advertisements and recommendations as well as more onerous transparency, and platform accountability requirements for those classified as VLOPs / VLSEs. For example, while Malaysia's Draft Code requires companies to perform regular 'audits', only the DSA specifically requires VLOPs / VLSEs to conduct an independent audit annually and appoint a dedicated compliance officer responsible for managing DSA requirements.



# What does this mean for internet companies operating in Malaysia?

Companies that fall directly in scope of the requirements will need to locally incorporate in Malaysia, to meet the licensing requirements. This is likely to present challenges for foreign-based companies, in terms of tax and legal implications, legal entity structuring, broader compliance with corporate laws and all the related costs associated with incorporation including administrative expenses, and initial setup costs.

Additionally, companies will need to ensure they have the appropriate systems in place to monitor and remove harmful content, including appointment of a local content moderation team. They will also need to have infrastructure in place to support reporting, respond to user reports and flags, and establish and enforce clear limits on the use of personal data in advertising.

The requirements related to conducting risk assessments will also necessitate the development of policies, risk models and related monitoring and reporting systems. All of which will require the implementation of appropriate governance, oversight and controls.

Companies that are not yet within scope of the framework, will also have to consider if expansion within the Malaysian market will lead to future licensing requirements or if the MCMC will expand the scope of application at a future date and what this will mean for their business.

Nevertheless, three of the five companies that are likely to fall within-scope of the Malaysia requirements are also designated as VLOPs / VLSEs under the DSA and four of the five companies have an organisation within their Group structure designated as such. Therefore, there should be some opportunities to leverage the strategies, policies, frameworks, processes, and learnings from other parts of the organisation already subject to the DSA and DMA requirements.





# How can we help?

Deloitte has strong global capabilities on digital regulation and we have supported several large global companies with the implementation of DSA, DMA, and other regulations impacting online platforms and services. We work closely with digital regulation experts across Deloitte Global, leveraging specialists from across our businesses including tax, legal, consulting and audit to deliver end-to-end regulation driven services. We understand the complexities and challenges global platforms face when navigating new regulatory frameworks. Our team of experts is equipped to provide comprehensive support in the following areas:

1

### Compliance Assessment:

We conduct in-depth assessments to determine whether your platform meets the regulatory requirements and provide practical solutions to comply with the obligations under the CMA.

2

### ASP(C) License Application Assistance:

Our team can guide you through the licensing process, ensuring that your application is completed accurately and submitted on time to avoid penalties.

3

### Target Operating Model (TOM):

We can support the development and optimise the TOM design and implementation for compliance capabilities across the three lines of defense.

4

### Post-Licensing Support

(Ongoing Compliance, Risk Management Assessments and Reporting):

Once licensed, we help service providers maintain compliance with the ASP(C) License obligations, including instituting the necessary controls and safeguards in place covering **content moderation, user safety protocols**, and assisting to prepare the template for **reporting** to the MCMC. We can also support the production of compliance reports as well as with implementing systemic risk assessments including methodology, execution and drafting of reports.





## Contact Us

To discuss how we can assist your organisation in meeting these requirements and ensure continued compliance with Malaysia's evolving digital regulations, please reach out to:

**Justin Ong**

Regulatory & Financial Risk Leader

Deloitte Southeast Asia

[keaong@deloitte.com](mailto:keaong@deloitte.com)

# Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

#### **About Deloitte Malaysia**

In Malaysia, services are provided by Deloitte Business Advisory Sdn Bhd and its affiliates.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.