



Southeast Asia
Public Policy Institute

Digital Platform Regulation in APEC Economies

Empowering Innovation and Inclusive Growth

A Policy White Paper, September 2025



This paper has been researched and produced by the Southeast Asia Public Policy Institute with support from ACT | The App Association. The information and analysis presented are based on interviews with relevant stakeholders, publicly available information, and analysis by the authors. It does not represent the views of The App Association. It is not intended to be an exhaustive review of policy, legislation, or regulation and should be used with due caution and consideration of its scope and limitations.

About the Southeast Asia Public Policy Institute



The Southeast Asia Public Policy Institute is a research institute based in Bangkok and Singapore, working across the region. Our mission is to support the development of solutions to the most pressing public policy challenges facing Southeast Asia in the 21st century. The Institute works on a range of issues across sustainability, technology, public health, trade, and governance.

We convene dialogues with stakeholders and decision makers to drive discussion on the challenges and opportunities facing markets in the region. The Institute draws on a network of in-market researchers, advisors, and partners to provide insights and recommendations for governments, policymakers, and businesses.

We collaborate with partners on projects to explore and drive discussion on policy challenges through:

- Research and Policy Development

In-depth research providing insights and actionable policy solutions aimed at policymakers looking to move the needle on key issues.

- Policy Dialogues and Roundtables

Present policy ideas and start a dialogue with the most relevant stakeholders holding the pen on policy development in markets across the region.

EXECUTIVE SUMMARY

The Asia-Pacific is one of the fastest-growing digital economies in the world, with Southeast Asia at its core. By 2023 the region's internet economy exceeded USD 200 billion and is projected to pass USD 300 billion in 2025, powered by e-commerce, ride-hailing, food delivery, fintech, and digital content. Large online platforms have become essential infrastructure for commerce, logistics, payments, and social interaction. This growth has created extraordinary opportunities for micro, small, and medium-sized enterprises (MSMEs), which account for over 98 percent of businesses and contribute 40–60 percent of GDP across APEC. Yet the systemic role of platforms has also raised concerns around competition, consumer protection, privacy, and market fairness, prompting calls for more structured regulation.

The European Union has taken an ambitious approach to digital regulation through its Digital Markets Act (DMA), Digital Services Act (DSA), and General Data Protection Regulation (GDPR). Together these instruments establish binding conduct rules for digital market “gatekeepers,” impose systemic safety and transparency duties, and harmonize privacy protections. Their extraterritorial reach and the so-called “Brussels Effect” give them global influence, shaping platform design choices well beyond Europe. Other jurisdictions have chosen different paths: the United Kingdom has tailored duties through its Digital Markets and Online Safety Acts which are independent if similar to the EU rules, the United States relies on litigation-driven antitrust enforcement and Section 230 protections, while China adopts a state-centric model linking content control, cybersecurity, and data localization. These contrasting approaches reveal that there is no global consensus on platform regulation, though there is a growing desire to consider regulatory intervention in the platform economy.



Across APEC, approaches vary widely. Emerging Regulatory Economies such as Indonesia, Malaysia, Thailand, the Philippines, and Vietnam rely primarily on general competition, consumer, and data laws, supplemented by targeted platform obligations such as registration, seller verification, takedown powers, and privacy regimes. The emphasis is incremental and adaptive, focused on accountability without imposing *ex ante* gatekeeper codes. Advanced Regulatory Economies including Singapore, Japan, South Korea, and Australia pair mature infrastructure with stronger institutional capacity. They have introduced more targeted rules, such as Japan's app-store transparency law, Korea's in-app billing choice mandate, Australia's Online Safety regime and proposed platform conduct codes, and Singapore's cross-border data and online-safety frameworks. Common threads are emerging around transparency, privacy, and MSME protection, but thresholds, remedies, and scope remain fragmented.

The EU's DMA is often seen as the most ambitious model of *ex ante* regulation, mandating non-discrimination, limits on tying, interoperability and portability, and user choice defaults. Its implementation in Europe has produced both promise and pitfalls: new rights for business users, alternative payment channels, and interoperability pilots have been accompanied by compliance complexity, fragmented user experiences, and safety trade-offs such as the appearance of unmoderated content in third-party app stores. For MSMEs, expanded data access and distribution options coexist with higher costs and trust gaps. These lessons suggest that while the DMA highlights real pressure points—ranking neutrality, payment steering, defaults, and data use—it is unclear whether its remedies will adequately address these issues and its mechanics demand substantial regulatory capacity and technical auditing. Wholesale transplantation into APEC would risk high compliance costs and potentially unintended harm both to innovation and to smaller firms in particular.



The policy challenge for APEC is to balance contestability, fairness, and trust with the need to sustain innovation and inclusive growth. Overly rigid algorithm rules could discourage platforms from improving quality, while broad data-access mandates might overwhelm MSMEs with compliance burdens. Bundling and defaults, often criticized in Western debates, can deliver real convenience and inclusion in fragmented Asian markets. Switching costs, often targeted by interoperability mandates, are already mitigated by widespread multi-homing behaviour in the region, reducing the need for intrusive design rules. Regulatory capacity also varies significantly, with advanced economies able to pilot targeted conduct regimes, while emerging economies benefit more from incremental co-regulatory approaches.

Quantifying the economic impact in APEC economies

To ground the assessment in evidence, we undertook quantitative analysis of potential compliance costs if DMA-style obligations were applied across APEC economies. Using platform-mediated e-commerce, digital advertising, and app distribution as the core channels, the modelling shows that in a medium scenario compliance costs would reach about USD 3.07 billion annually—equivalent to 0.02 percent of the combined GDP of nine economies. While modest in macroeconomic terms, the distributional effects are stark: roughly 70 percent of the burden, or USD 2.15 billion, would fall on MSMEs. In emerging economies where platforms are the main route to market, these costs translate into real frictions for small firms, tightening margins, slowing onboarding, and discouraging investment in growth. The analysis underscores that the “fit” question is not about headline GDP impact but about who pays, with disproportionate strain on the very businesses platform regulation is meant to empower.

Recommendations for APEC policymakers

- **Ground rules in evidence and proportionality:** Focus on demonstrated harms and avoid blunt size-based thresholds like those in the EU’s DMA. Obligations should scale with impact to prevent smaller firms from bearing disproportionate costs.
- **Engage inclusively:** Build rules through structured consultations with MSMEs, developers, platforms, and consumers. For example, advisory councils or industry roundtables can flag practical concerns early and prevent rules that unintentionally raise barriers for small businesses.
- **Use flexible tools:** Pilot measures in regulatory sandboxes (e.g. testing data portability features or algorithmic transparency disclosures) before mandating them economy-wide. Phased rollouts and safe harbours can ease adjustment, especially for smaller operators.
- **Ensure coherence across domains:** Coordinate competition, privacy, consumer protection, and online safety mandates to avoid duplication. For instance, aligning takedown timelines with data-protection obligations prevents conflicting compliance demands.
- **Support MSME participation:** Establish ombudsman offices or dispute-resolution portals to help MSMEs resolve conflicts with platforms quickly. Provide compliance templates and training so small firms can meet baseline standards without heavy legal costs.
- **Promote regional compatibility:** Develop shared definitions (e.g. what counts as self-preferencing), procedural standards (such as service-level agreements for handling appeals), and core transparency templates (e.g. ad disclosures). Mutual recognition of audits or certifications could reduce redundant costs across markets.
- **Embed review and adjustment:** Monitor indicators such as MSME onboarding costs, dispute outcomes, and cross-border compliance burdens. Regular regional reviews—through an APEC “state of digital markets” report—would allow obligations to be recalibrated based on evidence, scaling up what works and discarding what does not.

In sum, digital platforms have flourished in APEC under relatively light-touch rules, driving growth and empowering MSMEs. The region’s task now is to update its frameworks in a way that preserves these gains while addressing genuine risks. By resisting one-size-fits-all imports, sequencing interventions carefully, and prioritizing proportionate and regionally compatible approaches, APEC can build a smart regulatory pathway that safeguards fairness and trust without undermining the inclusive digital growth that has become one of its greatest successes.

CONTENTS



8-13

1. Understanding Digital Platforms & Emerging Regulatory Needs



14-22

2. Global Approaches to Platform Regulation



23-36

3. Platform regulation in APEC Economies



37-43

4. Policy focus: Adoption and adaptation of DMA-inspired policy in APEC Economies



44-51

5. Analysis: Assessing the regulatory fit for APEC economies



52-60

6. Policy Recommendations — Pathways to Smart Platform Regulation



UNDERSTANDING DIGITAL PLATFORMS

The Asia-Pacific region is one of the fastest-growing digital economies in the world. In Southeast Asia alone, the gross merchandise value of the internet economy surpassed USD 200 billion in 2023 and is projected to exceed USD 300 billion by 2025, driven by rising internet penetration, expanding mobile connectivity, and increasing adoption of digital payments. E-commerce, ride-hailing, online food delivery, and fintech services have become deeply embedded in daily life, while social media and digital content platforms have reached mass-market scale. This rapid expansion has attracted global platform operators, intensified competition with local players, and created a diverse set of regulatory challenges ranging from competition and consumer protection to cross-border data governance.

Large online platforms have become critical infrastructure for the digital economy, enabling commerce, logistics, payments, social interaction, and content distribution. While subject to general laws on competition, consumer protection, labour, and data governance, platforms operated for much of the early 21st century under a mix of self-regulation and legal frameworks not designed for their scale or business models. This has brought significant benefits to consumers and partners, in particular micro, small, and medium-sized enterprises (MSMEs). Across APEC, MSMEs make up more than 98 percent of enterprises, employ the majority of the workforce, and contribute between 40 and 60 percent of GDP.¹²³ Their ability to leverage digital platforms for payments, logistics, and new market access has been one of the most tangible dividends of light-touch regulatory approaches. Nevertheless, dissatisfaction with the limits of these arrangements by some has driven a shift in the 2020s toward updating existing rules and introducing platform-specific measures across competition, content, data, and worker rights.

The term “platform regulation” is not universally defined. Some argue that existing sectoral laws suffice, but regulators are increasingly finding early internet-era rules inadequate for addressing the systemic role of today’s platforms. For this paper, platform regulation refers to legal and policy instruments that explicitly or implicitly target online platforms or the platform economy, excluding generic data protection and e-commerce laws unless integrated into broader platform-focused frameworks.

Against this backdrop, approaches to platform regulation vary widely across jurisdictions, reflecting differences in market maturity, regulatory capacity, and policy priorities. In Emerging Regulatory Economies (ERE) such as Indonesia, Malaysia, Thailand, the Philippines, and Vietnam, rapid digital growth is intersecting with evolving governance frameworks, creating both opportunities and risks. Understanding these contexts is essential for assessing how global regulatory trends might be adapted to Southeast Asia’s unique economic and institutional landscape. In more mature markets in the region there are similar debates unfolding, though approaches vary.





1.1 EMERGING REGULATORY ECONOMIES (ERE)

Emerging Regulatory Economies (Indonesia, Malaysia, Thailand, the Philippines, and Vietnam) are central to Southeast Asia's digital expansion. Home to a young, tech-savvy population of roughly half a billion, these markets are driving Southeast Asia's rapid digital expansion. A key driver behind this growth is the abundance of youth and tech-savvy individuals. With a median age of approximately 30, Southeast Asia serves as a cradle for digital natives who are highly engaged online.⁴ This surge in digital adoption is further enabled by widespread access to affordable smartphones and fast internet connectivity.

The platform economy is anchored by a few well-defined growth sectors. E-commerce remains the anchor sector, providing sellers with access to demand, trust mechanisms, and fulfilment options that would otherwise require significant fixed investment. Mobility and on-demand services have expanded from urban transport to integrated delivery and logistics, enabling same-day and next-day commerce beyond capital cities. Digital financial services—wallets and instant account-to-account transfers—have broadened participation by lowering transaction frictions and expanding access to working capital. Finally, software-as-a-service and cloud-delivered tools are diffusing enterprise-grade capabilities to smaller firms. These sectors reinforce one another, with logistics, payments, and analytics improvements driving further adoption.⁵

The widespread and habitual use of smartphones underpins the mobile-first nature of Southeast Asia's digital transformation. Consumers in the region are some of the most engaged digital users globally, often active across a greater number of platforms than the global average.⁶ This breadth of usage underscores how deeply integrated digital platforms have become in everyday life—covering communication, entertainment, shopping, finance, and services—while also complicating trust-and-safety oversight and content regulation. This also raises a question as to whether any individual platform raises to the level of a “gatekeeper”, and whether laws placing specific requirements on gatekeepers is necessary.

At the same time, MSMEs are increasingly being drawn into the digital economy. Governments across Southeast Asia have prioritized the digitization of MSMEs as a national development goal. Public policies support the adoption of digital tools for payments, logistics, advertising, and cloud-based business management. These efforts are helping businesses not only streamline operations but also reach wider audiences and participate more effectively in platform-driven markets. As digital platforms provide ready-made infrastructure for commerce, more MSMEs are finding that they can scale with minimal upfront investment, further accelerating inclusive digital growth. Recent analysis by the Information Technology and Innovation Foundation (ITIF) underscores this trend, showing how digital services—from cloud solutions to e-commerce platforms—empower MSMEs and start-ups to innovate, expand, and compete in global markets.⁷

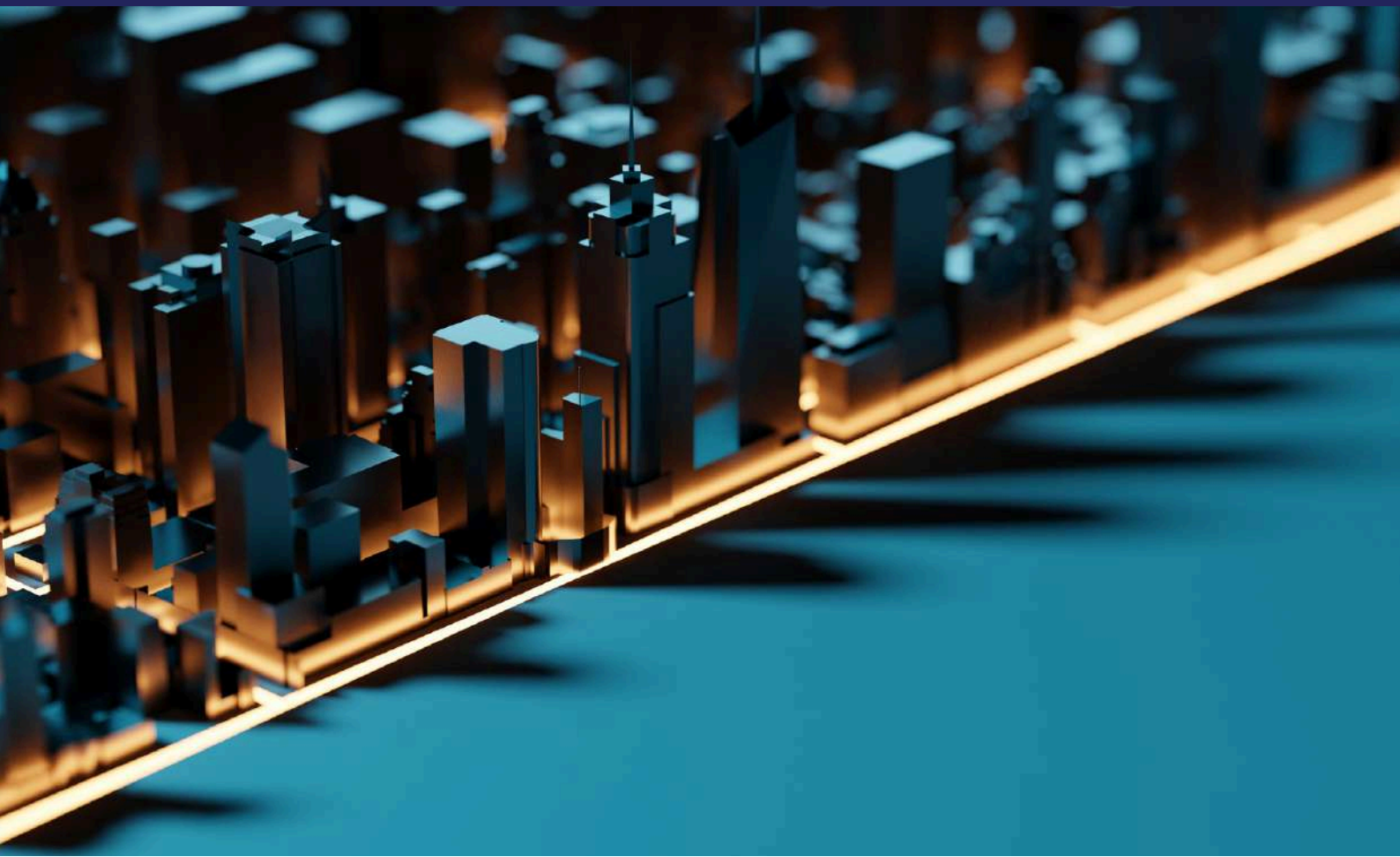
Several enablers have supported the scale of Southeast Asia's digital economy. Expanding logistics networks, instant payment systems, and affordable cloud services have lowered transaction costs and made digital participation easier for both consumers and MSMEs.⁸ At the same time, structural frictions remain. Cross-border payments and tax treatment are fragmented, skills and trust-and-safety capacity lag demand, and content moderation in local languages can be uneven.⁹ These conditions matter for regulation because platform rules interact directly with operational systems such as payments, logistics, and app-store distribution. The way rules are designed can influence costs, discovery, and participation, especially for smaller firms. These dynamics are examined in greater detail later in the paper.

Regulatory posture in EREs remains incremental. Competition authorities generally rely on ex post enforcement, using market studies and investigations to build evidence before introducing new rules. While antitrust agencies have examined marketplace conduct, exclusivity, and discrimination cases, there are no economy-wide platform codes in force. Moreover, consumer and e-commerce regulation has become the primary lever for accountability. Indonesia, Vietnam, and the Philippines have introduced seller-verification duties, takedown powers, and complaint-resolution mechanisms, raising baseline standards without targeting gatekeepers directly. These measures establish minimum safeguards for fairness and transparency while preserving flexibility for platforms and MSMEs.

Privacy and content governance frameworks are advancing in parallel. Recent data protection laws in Indonesia, Thailand, Malaysia, and Vietnam impose clearer obligations on platforms, while sectoral decrees on registration and moderation give authorities practical levers over digital services. Together, these instruments form the foundation of platform oversight, with further measures expected to evolve gradually as institutional capacity and market evidence develop.

Subsection 1.2 turns to the advanced regulatory economies of Singapore, Japan, South Korea, and Australia, highlighting their mature infrastructure, stronger regulatory capacity, and active oversight. This profile provides a reference point for the global frameworks in Section 2 and the comparative analysis that follows.





1.2 ADVANCED REGULATORY ECONOMIES (ARE)

The advanced regulatory economies in the region—Singapore, Japan, South Korea, and Australia—begin from a different baseline. These markets pair mature digital infrastructure and high adoption with stronger institutional capacity in privacy, competition, and consumer protection. Oversight of platform activity is active and relatively granular, addressing marketplace conduct, data mobility initiatives, transparency reporting, and audit mechanisms. In practice, authorities emphasise targeted conduct expectations and the promotion of technical portability to support contestability and user choice, alongside measures that strengthen trust, safety, and operational resilience.¹⁰

Regulatory posture and priorities share several features. First, supervision often combines ex-post enforcement with sector- or service-specific obligations where concentrated intermediation creates distinctive risks. Second, data portability and interoperability are used as pro-competitive tools intended to reduce switching costs and foster choice. Third, auditability and transparency are increasingly embedded in oversight, through reporting requirements, system documentation, and in some cases independent assurance. Finally, trust and safety considerations are advanced through codes of practice, online-safety rules, and governance pilots, with sandboxes or voluntary standards used to calibrate measures as technologies and business models evolve.¹¹

Cross-cutting challenges persist. Market contestability and fair access remain live issues in concentrated ecosystems and super-app environments, with periodic concerns about barriers to entry or perceived preferential treatment. Updating privacy frameworks while supporting responsible reuse and portability requires careful calibration to avoid unintended constraints on innovation or data sharing in the public interest. A further tension lies in sustaining startup dynamism while maintaining high compliance standards, particularly in hub markets where young firms are sensitive to the predictability and administrative cost of rules and processes.¹²

Country experience illustrates these patterns without being uniform.

- Singapore pairs mature governance and active competition and consumer oversight with digital-trade frameworks that emphasise trusted cross-border data flows and governance pilots in emerging technologies.¹³¹⁴
- Japan anchors policy in a comprehensive privacy regime and national digital-identity infrastructure alongside initiatives to accelerate MSME digital adoption and strengthen cybersecurity.¹⁵¹⁶
- South Korea combines extensive connectivity and super-app ecosystems with active competition oversight; debates over contestability, preferential treatment of domestic firms, and market access continue alongside initiatives on portability and app-distribution conduct.¹⁷¹⁸
- Australia expands data mobility through consumer-initiated data sharing, sustains competition authority scrutiny of digital platforms, and advances privacy reform and online-safety measures, reflecting a willingness to deploy sectoral codes and targeted obligations.¹⁹²⁰

Platforms thus operate against different starting conditions in the ERE and ARE groups. Across both, the operational channels through which rules affect participation are clear: discovery and ranking, distribution terms, access to performance data, and switching frictions. Section 2 introduces the principal global approaches that target these channels, with particular emphasis on frameworks for market conduct, online safety, and data protection. That overview provides the common vocabulary needed for the comparative assessment that follows.



GLOBAL APPROACHES TO PLATFORM REGULATION



THE EUROPEAN UNION'S APPROACH

Global regulators have increasingly focused on large digital platforms, such as online marketplaces, social networks, and app stores, because of their outsized influence on markets and society. The European Union has established itself as the prime mover on digital regulation. Through the so-called “Brussels Effect,” stringent EU rules have resonated beyond their borders as multinational companies adjust operations worldwide to comply, despite there being active debate over whether the EU is taking the best approach. The EU’s laws also have explicit extraterritorial reach: companies offering services to EU users must comply regardless of where they are based. This combination gives EU initiatives substantial spillover impact—non-EU businesses align practices to keep serving the EU market, and many governments emulate EU frameworks in their own legislation even if the EU approach is not always the best approach for the local context.

Nowhere is this clearer than in competition, content, and privacy policy: the EU has been the first to codify ex ante rules for platform conduct, systemic obligations for online safety, and harmonised data protection standards. The following sections examine these three pillars—the Digital Markets Act (DMA), the Digital Services Act (DSA), and the General Data Protection Regulation (GDPR)—each targeting different facets of the digital economy.



Competition in Digital Markets: The EU Digital Markets Act (DMA)

The Digital Markets Act (DMA) is the European Union’s most ambitious initiative to date in addressing the market power of large technology firms. First proposed by the European Commission in December 2020, it was adopted by the European Parliament and the Council in September 2022, entered into force on 1 November 2022, and became applicable from 2 May 2023.²¹ It establishes an ex ante regulatory framework designed in theory to ensure fair and contestable digital markets by imposing binding conduct requirements on a small group of highly influential companies—termed “gatekeepers.”

Under Article 3 of the DMA, a company is designated as a gatekeeper if it:²²

1. Has achieved an annual EU turnover equal to or exceeding €7.5 billion in each of the last three financial years, or an average market capitalisation (or equivalent fair market value) of at least €75 billion in the last financial year.
2. Provides at least one “core platform service” in at least three EU Member States
3. Serves more than 45 million monthly active end-users established or located in the EU, and more than 10,000 yearly active business users established in the EU, in each of the last three financial years.



Core platform services, as defined in the regulation, include online intermediation services (such as app stores), online search engines, social networking services, video-sharing platform services, number-independent interpersonal communication services (such as messaging applications), operating systems, cloud computing services, web browsers, virtual assistants, and online advertising services.²³

The European Commission announced the first set of gatekeeper designations in September 2023, covering both companies and the specific core platform services they operate.²⁴ The Commission retains the authority to update the list through market investigations to address changes in market structure or emerging business models.

The DMA sets out a detailed rulebook of permissible and prohibited conduct that designated gatekeepers must implement within six months of designation. In addition to prohibiting self-preferencing in rankings and search results, the regulation requires gatekeepers to offer business users fair, reasonable, and non-discriminatory access to their core platform services, and to refrain from making the use of one service conditional upon the adoption of another, such as mandating a proprietary payment system. Business users must be allowed to promote offers and conclude contracts with customers outside the gatekeeper’s platform without penalty, and end-users must be able to uninstall preloaded applications and switch default settings without undue friction. The DMA also obliges gatekeepers to facilitate interoperability between their core platform services and third-party services, including progressive interoperability for messaging, and to grant advertisers and publishers access to the performance measurement tools and data needed for independent verification of advertising metrics.²⁵

Gatekeepers are further required to ensure data portability, provide business users with access to the data they generate through the platform, and refrain from using non-public data from business users to compete against them. They may not combine personal data from different core platform services or with data from third-party services without the user's explicit consent, and they must ensure interoperability for hardware and software features such as operating systems and virtual assistants. In addition, gatekeepers must inform the European Commission of all intended acquisitions or mergers involving digital services, irrespective of whether these transactions meet standard EU merger control thresholds.²⁶ Any combination of personal data, advertising practices, or technical integration must comply fully with applicable privacy and data protection laws.

Enforcement is proactive rather than reactive. The Commission directly supervises compliance, has the power to conduct audits and investigations, and may impose administrative fines of up to 10 per cent of global turnover—or 20 per cent for repeated infringements.²⁷ In cases of systematic non-compliance, structural remedies may be imposed.²⁸ The success of the DMA is not assured and will depend on the operational feasibility of certain obligations, such as the practical implementation of interoperability or the definition of unlawful self-preferencing. More importantly, it will be judged on whether its effects lead to better opportunities and competition, something that is not guaranteed.

Although the DMA is the EU-wide solution, it did not emerge in a vacuum. Germany moved first at national level: on 19 January 2021 the 10th amendment to the Act against Restraints of Competition introduced Section 19a, an ex-ante tool enabling the Bundeskartellamt to designate firms of “paramount significance across markets” and impose targeted obligations. The DMA has since become a touchstone for other jurisdictions. The United Kingdom's Digital Markets, Competition and Consumers Act received Royal Assent on 24 May 2024, and its digital-markets regime took effect on 1 January 2025, empowering the CMA to designate companies with Strategic Market Status and set binding conduct requirements. Japan followed in June 2024 with the Act on Promotion of Competition for Specified Smartphone Software—an ex-ante regime narrowly focused on mobile operating systems, app stores, browsers and search—scheduled to enter into force by Cabinet order within eighteen months of promulgation. Together these approaches represent a proactive, conduct-based oversight of large platforms.

Yet the DMA should not be mistaken for a global consensus. Even within the EU, policymakers and businesses continue to debate on whether the DMA is the right approach. Beyond Europe, approaches diverge markedly. The United States has emphasized antitrust enforcement through litigation rather than ex-ante codes, while China's framework is grounded in state oversight of data and security. This diversity underscores that while the DMA is highly influential, it is neither universally endorsed nor easily transplantable. Nevertheless, because compliance obligations fall on global firms, many of the changes the DMA catalyses (for example, alternative in-app payments and enhanced data access for business users) may spill over into other markets, including APEC, even where regulators pursue different models.²⁹

Online Content Regulation and Safety: The EU Digital Services Act (DSA)

The Digital Services Act (DSA) is the European Union’s modernised framework for regulating online intermediaries and platforms, designed to enhance user safety, ensure transparency, and protect fundamental rights in the digital environment. Proposed by the European Commission in December 2020 alongside the DMA, it was adopted by the European Parliament and Council in October 2022, entered into force on 16 November 2022, and became applicable from 17 February 2024. For the largest platforms and search engines—designated as “Very Large Online Platforms” (VLOPs) and “Very Large Online Search Engines” (VLOSEs)—most obligations took effect earlier, from 25 August 2023.³⁰

The DSA applies to a broad spectrum of services, including intermediary services (such as internet service providers), hosting services (including cloud storage), online platforms (such as social media or marketplaces), and online search engines. It introduces graduated obligations proportionate to the size, reach, and societal impact of the service.

VLOPs and VLOSEs are defined as having an average of more than 45 million monthly active users in the EU—equivalent to 10 per cent of the EU population—calculated over the preceding six months.³¹ The European Commission maintains a public list of designated VLOPs and VLOSEs, which as of 2024 covers 19 services operated by a range of major global technology companies.³²

The DSA establishes a layered set of requirements. All intermediary services must have a single point of contact for users and authorities, publish clear terms of service, and cooperate with national authorities. Hosting services must provide mechanisms for users to flag illegal content, act expeditiously on valid notices, and give reasons for any content removal or account suspension. Online platforms are further required to provide internal complaint-handling systems, offer access to independent out-of-court dispute resolution, and publish detailed transparency reports. They must also implement “Know Your Business Customer” procedures to verify the identity of traders and inform users when they are interacting with a business seller.³³



VLOPs and VLOSEs face the most stringent obligations. They must conduct annual systemic risk assessments covering illegal content, the dissemination of disinformation, impacts on electoral processes, gender-based violence, protection of minors, and other threats to fundamental rights. They are required to implement effective mitigation measures, submit to independent annual audits, and provide vetted researchers with access to platform data under safeguards. They must also give users greater control over recommender systems, including an option not based on profiling, and are prohibited from using sensitive personal data for targeted advertising or showing any targeted advertising to minors.³⁴

The European Commission directly supervises VLOPs and VLOSEs, while national Digital Services Coordinators oversee other services. Non-compliance can result in fines of up to 6 per cent of global annual turnover, and periodic penalty payments may reach up to 5 per cent of the average daily turnover.³⁵ In serious cases, the Commission can request that a court suspend the provision of services in the EU.

The DSA's transparency, accountability, and systemic-risk toolkit has been adopted in some respects elsewhere—backed by fines up to 6% of worldwide turnover and, more recently, a July 2025 delegated act operationalising researcher data access. Subsequent regimes have moved in parallel or further: the UK's Online Safety Act (Royal Assent 26 October 2023) is phasing in across 2024–25 with penalties up to the higher of £18 million or 10% of qualifying worldwide revenue, and Australia's Online Safety Act has been in force since 23 January 2022, underpinned by “Basic Online Safety Expectations” set by the eSafety Commissioner. In practice, this convergence means large platforms often roll out DSA-style features—such as non-profiled recommender options, strengthened notice-and-action, and enhanced transparency reporting—globally for operational consistency, even as success is also not assured turns on multilingual moderation, robust auditing, and meaningful researcher access.



Data Protection and Privacy Standards: The EU GDPR

The General Data Protection Regulation (GDPR) is the European Union's comprehensive data protection framework, designed to harmonise privacy rules across Member States and strengthen individuals' control over their personal data. Proposed by the European Commission in January 2012, adopted in April 2016, and applicable from 25 May 2018, it replaced the 1995 Data Protection Directive and introduced a directly applicable regulation with extraterritorial reach.³

The GDPR applies to any organisation—regardless of location—that processes personal data of individuals who are in the EU, where the processing relates to the offering of goods or services or the monitoring of behaviour within the EU.³⁷ It establishes a set of core principles for lawful processing, including purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. A lawful basis for processing must be established, such as consent, contractual necessity, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest, or legitimate interests pursued by the controller.³⁸

The regulation grants data subjects a suite of rights, including the right of access, rectification, erasure (“right to be forgotten”), restriction of processing, portability of their data to another controller, objection to certain processing, and safeguards against automated decision-making and profiling.³⁹ Controllers must provide these rights in a timely and accessible manner. Transparency obligations require clear privacy notices, and significant processing activities—particularly those involving high-risk operations—must be documented and, in some cases, subjected to a Data Protection Impact Assessment (DPIA).⁴⁰


The GDPR also imposes organisational and technical measures for compliance. Certain entities must appoint a Data Protection Officer (DPO), maintain records of processing activities, and implement security measures appropriate to the level of risk. Personal data breaches must be notified to the relevant supervisory authority within 72 hours of discovery, unless unlikely to result in risk to rights and freedoms, and to affected data subjects without undue delay when there is a high risk. Cross-border data transfers are restricted to jurisdictions deemed “adequate” by the European Commission or must be safeguarded by mechanisms such as Standard Contractual Clauses or Binding Corporate Rules.⁴¹

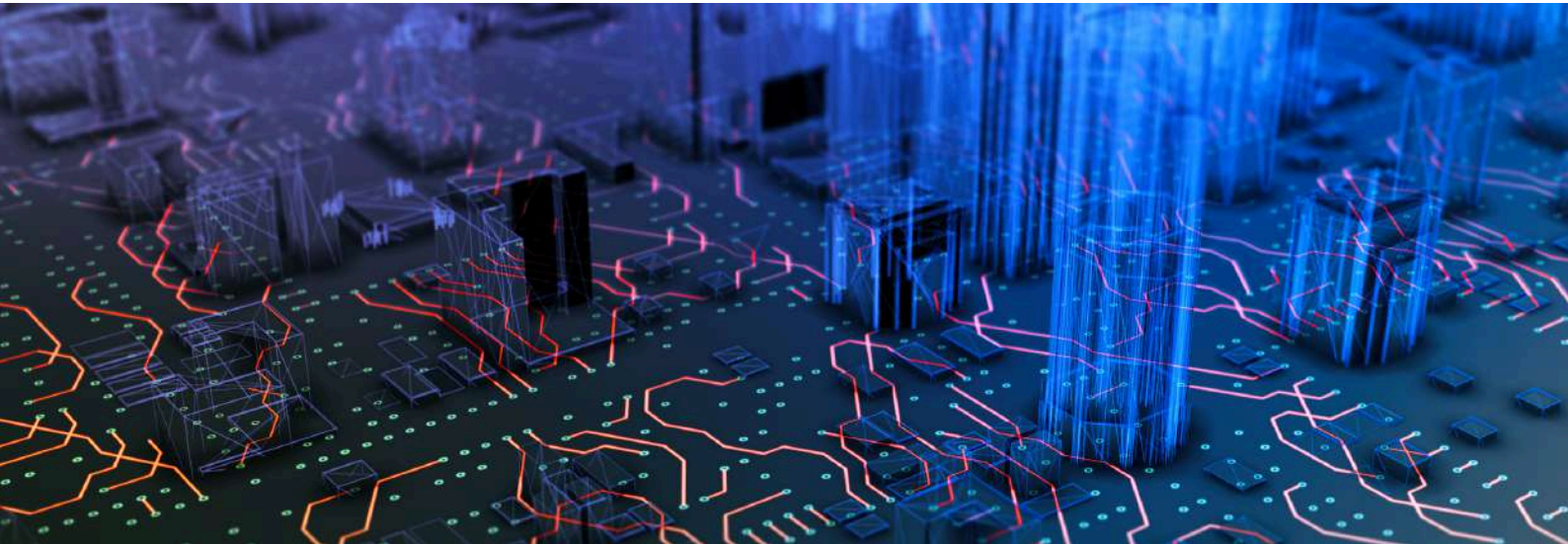
Enforcement is carried out by independent national Data Protection Authorities (DPAs), coordinated through the European Data Protection Board. Administrative fines can reach up to the higher of €20 million or 4 per cent of the total worldwide annual turnover of the preceding financial year, depending on the severity of the infringement. Lesser infringements may result in fines of up to €10 million or 2 per cent of turnover.⁴² DPAs may also issue reprimands, impose bans on processing, or order corrective actions.



Since 2018, the GDPR has become the de facto global baseline: by 2025, 144 countries have enacted national data-privacy laws—covering roughly 82% of the world’s population—many borrowing GDPR-style principles and rights. The EU’s “adequacy” club has also expanded: as of July 2025, the Commission has adopted adequacy decisions for 16 jurisdictions (including the EU–U.S. Data Privacy Framework for certified U.S. firms and the European Patent Organisation), extending GDPR-level protections through trusted data-flow arrangements. This diffusion means multinationals frequently apply GDPR-level controls globally. Within the EU’s regulatory framework, the GDPR interacts directly with the DMA and DSA: interoperability and data access requirements under the DMA, and advertising and recommender system transparency obligations under the DSA, must all be implemented in ways that are compatible with GDPR principles and protections. This integrated approach has made the GDPR a central pillar of Europe’s digital regulation model and a reference point for global privacy governance.

Other Jurisdictions’ Approaches

While the EU’s approach is the most comprehensive, other jurisdictions have pursued their own models. These vary in scope, enforcement style, and policy drivers.

Jurisdiction	Core Approach	Key Features
 United Kingdom	Modelled after the EU	<p>The UK’s approach to platform regulation is underpinned by two recent legislative pillars. The Online Safety Act 2023 establishes a comprehensive duty of care on online services to protect users from illegal content and, in certain cases, harmful but legal content, with the Office of Communications (Ofcom) empowered to enforce detailed codes of practice.⁴³ In parallel, the Digital Markets, Competition and Consumers Act 2024 creates a statutory Digital Markets Unit (DMU) within the Competition and Markets Authority⁴⁴, tasked with designating firms with “Strategic Market Status” and imposing tailored conduct requirements to address anti-competitive behaviour.⁴⁵</p> <p>While these measures reflect domestic priorities, they draw heavily from the EU’s Digital Services Act and Digital Markets Act in both structure and objectives, adapting them to a UK context through more bespoke, case-by-case obligations.⁴⁶</p>



Jurisdiction	Core Approach	Key Features
 United States	Pro-growth	<p>It is difficult to summarise the US approach to platform regulation as there are no specific platform laws. Competition issues are dealt with under existing anti-trust law, and content takedowns are rules by the DMCA.⁴⁷ There is a growing body of US state law that may fragment the landscape.⁴⁸ However, underpinning the approach is Section 230 of the Communications Decent Act which provides for broad immunity to online platforms for content posted by users. The fact that most major platforms are US-based has meant that this approach has been exported by proxy.⁴⁹ However, the Section 230 protections remain controversial with some stakeholders and this on-going debate can influence global discussions around platform accountability.⁵⁰</p>
 China	Pro-control	<p>China takes a strict approach to online content as well as data security, implemented through its Cybersecurity Law (2018), Data Security Law (2021) and regulations on online information dissemination.⁵¹⁵²⁵³ China's Anti-Monopoly Law (amended 2022) is not specific to online platforms but does address issues such as data dominance.⁵⁴ This approach can be an attractive model for countries seeking tighter control over their digital space. While the regulation is strict, it cannot be said that it has not fostered innovation, as China has one of the most dynamic online ecosystems in the world.⁵⁵</p>



PLATFORM REGULATION IN APEC ECONOMIES

This section presents a snapshot of the approaches to platform regulation in APEC economies, based around two tables outlining existing policies, legislation and regulation and policy pipeline.

3.1 EMERGING REGULATORY ECONOMIES (ERE)

DRAFT	Competition	Content Regulation	Data Protection
Indonesia	Law No. 5/1999 (general competition law); KPPU Reg. 3/2023 (merger control).	Kominfo Reg. 5/2020 on Private ESOs (registration, takedown duties).	Personal Data Protection Law No. 27/2022 (PDP Law)
		ITE Law (No. 11/2008, as amended by Law No. 1/2024).	Government Regulation No. 71 (2019)
Malaysia	Competition Act 2010.	Communications & Multimedia Act 1998 (statutory content powers).	Personal Data Protection Act 2010 (Act 709)
		Malaysian Communications & Multimedia Content Code (2022) (industry self-reg, registered by MCMC).	
Thailand	Trade Competition Act B.E. 2560 (2017).	Royal Decree on the Operation of Digital Platform Service Businesses (B.E. 2565/2022)	Personal Data Protection Act B.E. 2562 (2019) (in force since 2022)
	Draft Guideline on Unfair Trade Practices for E-commerce Platforms	Computer Crime Act B.E. 2550 (2007)	

- Platform-focused law
- Law with significant impact on platforms
- Voluntary or indirect rules, guidelines, codes
- Draft platform-focused law
- Draft law with significant impact on platforms
- Not platform-focused law

DRAFT	Competition	Content Regulation	Data Protection
Philippines	Philippine Competition Act (RA 10667).	Internet Transactions Act (RA 11967, 2023).	Data Privacy Act (RA 10173).
		Cybercrime Prevention Act (RA 10175).	
		The Anti-Financial Scamming Act (2024, awaiting IRR in 2025)	
Vietnam	Law on Competition No. 23/2018/QH14 (effective 2019)	Decree 147/2024 (replacing Decree 72) on internet services/online information (platform obligations)	Decree 13/2023/ND-CP on Personal Data Protection (PDPD)
		Law on Cybersecurity (2018) + Decree 53/2022 (data-localization, takedown)	Law on Data (2025)

- Platform-focused law
- Law with significant impact on platforms
- Voluntary or indirect rules, guidelines, codes
- Draft platform-focused law
- Draft law with significant impact on platforms
- Not platform-focused law

Source: Author’s compilation based on national legislation and regulatory instruments, including competition, content, and data protection laws and decrees in Indonesia, Malaysia, Thailand, the Philippines, and Vietnam.



Indonesia

Competition Oversight

Indonesia's approach is pragmatic and incremental, relying on general competition, trade, and sectoral rules rather than a single prescriptive platform statute. Oversight remains case-driven but increasingly assertive. The Indonesian Competition Commission (KPPU) has focused on marketplace dynamics and platform integrations, most visibly in conditionally clearing TikTok's acquisition of a 75.01% stake in Tokopedia (June 2025) with conduct conditions (non-discrimination in payments/logistics) and multi-year monitoring. Legislative initiatives, such as the draft Broadcasting Law and presidential action on publishers' rights, point to a broader willingness to extend oversight into adjacent digital sectors.⁵⁶ The overall direction is tighter scrutiny of platform conduct through existing tools rather than a separate, size-triggered rulebook.



Content Regulation

Platform governance centers on mandatory registration, expedited takedown, and technical-order powers, giving regulators practical levers over both domestic and global operators. Recent amendments to the Electronic Information and Transactions Law (ITE) framework expand the state's ability to direct content moderation and technical adjustments, with non-compliance carrying the risk of service disruption.⁵⁷ These tools provide flexibility to address new risks without creating sector-specific conduct prohibitions.

Data Protection

Data protection and digital trade rules are raising the baseline for compliance and transparency. With the Personal Data Protection Law now fully in force, platforms face clearer duties on governance, breach response, and processor oversight. Government Regulation No. 71 of 2019 (GR71) on the Operation of Electronic Systems also shapes obligations, requiring registration of electronic systems operators and setting conditions for cross-border data transfers. Trade regulations also separate social content from in-app payments, reinforce seller verification, and restrict direct offshore sales below a set threshold, all intended to safeguard domestic commerce and level the playing field for Indonesian businesses.⁵⁸



Malaysia

Competition Oversight

Malaysia's posture is size-based licensing plus updated competition, content, and privacy rules—assertive on accountability but still far developing an ex-ante conduct code. Since 1 January 2025, internet messaging and social media services with eight million or more Malaysian users must hold an ASP(C) licence, formalising local obligations for the largest platforms and giving the Malaysian Communications and Multimedia Commission (MCMC) clearer enforcement levers. In parallel, the Malaysia Competition Commission (MyCC) has stepped up scrutiny of digital markets: its 2024–25 priorities include monitoring app stores, online advertising, and marketplace conduct under the Competition Act 2010, alongside ongoing preparations for a revised Competition Act that would add a merger-control regime. Together these measures increase regulatory visibility of platform behaviour without yet creating sector-specific conduct obligations.⁵⁹

Content Regulation

Content enforcement has also been tightened through the Communications and Multimedia (Amendment) Act 2025, which expand investigatory powers and update offence provisions, including new restrictions on unsolicited electronic messaging. At the same time, the government has opted to delegate oversight of news content to an industry-led body under the Malaysian Media Council Act, signalling a preference for co-regulation in sensitive areas rather than direct state control. Together with enhanced competition scrutiny and the modernization of privacy law, these changes reinforce a trajectory toward greater platform accountability, though still short of the prescriptive, code-based models emerging in Europe.⁶⁰

Data Protection

Privacy modernization moved in parallel. The Personal Data Protection (Amendment) Act 2024 phased in during 2025 adds mandatory breach notification, data-protection officers, data portability, and an updated cross-border transfer regime (with new conditions and guidance on transfer-impact assessments).⁶¹ These changes raise the baseline for security and transparency and interact directly with licensing and platform reporting.





Thailand

Competition Oversight

Thailand's move toward ex-ante oversight is now anchored in existing instruments rather than a new statute. The Office of the Council of State advised in March 2025 that work on a standalone Platform Economy Act should be paused, and policy has shifted to tightening supervision under the Royal Decree regime and sectoral measures.⁶² Competition oversight is being sharpened through forthcoming Trade Competition Commission guidance for multi-sided and e-commerce platforms, while ETDA has begun using “high-risk” designations and targeted obligations (including new operational rules for online marketplaces effective 31 December 2025) to push proactive compliance.⁶³

Content Regulation

Thailand has consolidated content-moderation rules within the Ministry of Digital Economy and Society (MDES). A 24-hour takedown obligation upon official notice is now in force for specified social-media content, backed by enforcement powers under the Computer Crime Act and coordinated by MDES. ETDA's 2025 marketplace notification also layers transparency, reporting, and compliance-program duties on platforms, requiring internal procedures for content moderation and escalation. These measures reflect a more systematic approach to online content governance, emphasising rapid responsiveness and auditable moderation systems rather than a standalone publishers' law.

Data Protection

The regulatory framework for data privacy has matured with the full enforcement of the Personal Data Protection Act (PDPA). In 2025, the Personal Data Protection Committee announced several administrative fines, raising the compliance baseline for governance, incident reporting, and processor oversight. In parallel, data-gathering obligations under the Royal Decree require domestic and cross-border platforms serving Thai users to notify ETDA and file annual returns detailing services, transactions, revenues, and user metrics, enabling further supervisory requests for “large” operators. Since 1 January 2024, platforms meeting statutory thresholds must also maintain an electronic special account and report seller-level revenues to the Revenue Department, materially improving auditability of marketplace activity and tax enforcement., with multiple administrative fines announced, raising the baseline on governance, incident handling, and processor oversight.⁶⁴ There is no separate, platform-specific publishers' law; media issues continue to be handled through existing frameworks.



Philippines

Competition Oversight

The Philippines relies on competition law, consumer protection, and content statutes rather than a dedicated platform code, with emphasis on strengthening investigatory and supervisory capacity. The Philippine Competition Commission (PCC) has elevated digital markets to a priority area, producing a 2024 market study on platforms and online advertising and issuing guidance in 2023 for motu proprio reviews of technology mergers and acquisitions. Ongoing investigations increasingly probe marketplace practices, app-store conditions, and ad-tech measurement, signalling a more assertive posture even in the absence of ex-ante conduct rules.⁶⁵

Content Regulation

Consumer protection has been significantly bolstered through the Internet Transactions Act of 2023 (RA 11967), now fully in force with implementing rules and regulations. The law places internet-based merchants, marketplaces, and platforms under the Department of Trade and Industry (DTI), which is empowered to issue summons, subpoenas, compliance orders, and takedown or blacklist orders. The new E-Commerce Bureau leads implementation, while the introduction of a voluntary trustmark aims to build consumer confidence in online transactions. These measures position the DTI as a central regulator of digital commerce, moving beyond its traditional remit.⁶⁶



Data Protection

Content governance and trust-and-safety measures remain rooted in existing statutes. The Cybercrime Prevention Act, Anti-Terrorism Act, and Data Privacy Act together shape the obligations of digital platforms, with the National Privacy Commission overseeing privacy compliance. Identity verification and fraud prevention are reinforced by the SIM Registration Act, which requires registration of SIM cards to curb anonymous abuse. Proposals for a broader “online harms” framework have been debated but remain pending.⁶⁷



Vietnam

Competition Oversight

Vietnam's stance is structural but distributed: rather than a single omnibus platform statute, it layers scale-linked obligations across adjacent laws, singling out large and very large services for proactive duties. This approach disciplines platform conduct primarily through transparency, disclosure, and process requirements embedded in the Law on E-Transactions (2023, with a 2024 decree) and the updated Consumer Protection Law (2023). Very large services must disclose recommendation criteria in Vietnamese and provide opt-outs; marketplaces are obliged to archive advertising, explain ranking and prioritisation (including sponsored results), and strengthen procedures for fake-account handling and automated systems. While the Vietnam Competition Commission and the 2018 Competition Law remain central for ex-post cases, in practice platform behaviour is increasingly shaped by these scale-triggered obligations.⁶⁸

Content Regulation

Content governance was overhauled in December 2024, introducing stricter requirements for cross-border services. Providers meeting traffic or infrastructure thresholds must register a local contact point, comply with removal orders on official notice within defined timelines, store user data for disclosure, and implement account verification and repeat-offender locks. Offshore app stores are required to remove illegal applications and adhere to domestic payment rules, while authorities retain blocking powers. Platforms are also encouraged to cooperate with Vietnamese press agencies and to deploy automated detection against harmful content—expectations reinforced through regulatory inspections and remedial orders.⁶⁹

Data Protection

Privacy and data rules provide an additional compliance floor. The 2023 personal-data decree mandated impact assessments, stronger consent, and documentation for cross-border transfers, while the cybersecurity framework enables localisation orders requiring in-country storage and local establishment. The Law on Data, effective 1 July 2025, formalises a national data architecture and rules for sharing and protection, adding further obligations for both domestic and foreign platforms. Fiscal transparency has tightened in parallel: foreign suppliers must register and remit via the tax portal, and from 1 July 2025 platforms enabling payments must withhold, declare, and remit VAT and personal-income tax on behalf of individual and household sellers.⁷⁰



3.2 ADVANCED REGULATORY ECONOMIES (ARE)

	Competition	Content Regulation	Data Protection
Singapore	Competition Act 2004 (Cap. 50B) administered by CCCS; revised merger guidelines and digital market study (2020).	Online Safety (Miscellaneous Amendments) Act 2022 (amends Broadcasting Act, imposes obligations on social media platforms).	Personal Data Protection Act 2012 (amended 2020 for mandatory breach notification, higher fines).
		Codes of Practice (e.g. Protection from Online Falsehoods and Manipulation Act (POFMA, 2019); Code of Practice for Online Safety, 2023).	
Japan	Act on Improving Transparency and Fairness of Digital Platforms (2020) (covers app stores, e-commerce marketplaces).	Provider Liability Limitation Act (2001, amended 2021); Act on Development of an Environment for Ensuring Safe and Secure Internet Use by Youth (2008).	Act on the Protection of Personal Information (APPI), originally 2003, amended 2015, 2020, 2022 (extraterritorial application).
	Antimonopoly Act (AMA, 1947, as amended).	MIC/FTC digital platform guidelines.	
	Smartphone Act (2024) (enhancing app store payment choice and competition)		
South Korea	Online Platform Fairness Act (proposed 2021, not passed)	Telecommunications Business Act amendments (2021, net neutrality, app store billing rules)	Personal Information Protection Act (PIPA, 2011; overhauled 2020).
	Monopoly Regulation and Fair Trade Act (MRFTA, 1980, amended multiple times); Telecommunication Business Act (2021 amendment banning app store anti-steering).	Information and Communications Network Act (2001, amended)	

	Competition	Content Regulation	Data Protection
Australia	Competition and Consumer Act 2010 (Part IV).	Online Safety Act 2021 (establishes eSafety Commissioner; duties for social media, search, app stores).	Privacy Act 1988 (under review); Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 increased penalties.
	ACCC Digital Platforms Inquiry (2019) → News Media Bargaining Code (2021).	Industry codes under Broadcasting Services Act (e.g. misinformation/disinformation code, 2021).	
	Draft proposals for “ex ante” DMA-style obligations under consultation.		

- Platform-focused law
- Law with significant impact on platforms
- Voluntary or indirect rules, guidelines, codes
- Draft platform-focused law
- Draft law with significant impact on platforms
- Not platform-focused law

Source: Author’s compilation based on national legislation and regulatory instruments, including competition, content, and data protection laws and decrees in Singapore, Japan, South Korea, and Australia.

Singapore

Competition Oversight

Singapore has developed a mature and coordinated digital governance framework, combining competition, consumer, and data oversight within a pro-innovation policy environment. Rather than adopting prescriptive codes, regulators deploy targeted guidance, sectoral standards, and cross-border frameworks. Oversight is anchored in the work of the Competition and Consumer Commission of Singapore (CCCS), which monitors digital market practices ranging from app-store fairness to online consumer contracts. Updated guidelines and market studies have sharpened expectations around transparency and fairness in e-commerce, while creating conditions for enforcement to be proportionate and evidence-based. This case-led model allows Singapore to address anti-competitive risks without a separate platform statute.⁷¹



Content Regulation

Content and online safety are managed through existing instruments. The Protection from Online Falsehoods and Manipulation Act (POFMA) empowers authorities to direct corrections or removals of false content, while the Online Safety (Miscellaneous Amendments) Act of 2022 imposes obligations on major online services to limit exposure to harmful material. Codes of practice administered by the Infocomm Media Development Authority (IMDA), such as the Code of Practice for Online Safety, reinforce these statutory duties with operational requirements for transparency reporting, content moderation, and user safeguards.⁷²

Data Protection

Data governance is underpinned by the Personal Data Protection Act (PDPA), which establishes consent, purpose limitation, breach notification, and accountability requirements. Singapore has positioned itself as a leader in trusted cross-border data flows through Digital Economy Agreements and initiatives such as TradeTrust. The EU–Singapore Digital Trade Agreement enables free movement of data while maintaining GDPR-level safeguards, and Singapore continues to advance portability and interoperability through both domestic frameworks and international partnerships. In emerging technology, Singapore has opted for voluntary governance tools, such as the Model AI Governance Framework and the AI Verify testing toolkit, reflecting a strategy of building trust without constraining innovation.⁷³



Japan

Competition Oversight

Japan combines strong statutory safeguards with active state-led initiatives to accelerate digitalisation. Oversight is distributed across privacy, cybersecurity, and competition law, with policy priorities on digital identity, national security, and MSME adoption of technology. In 2021, Japan enacted the Act on Improving Transparency and Fairness of Digital Platforms, requiring major online malls and app stores to disclose ranking criteria, contract terms, and complaint mechanisms. In 2024, the Act on Promotion of Competition for Specified Smartphone Software was passed, addressing mobile operating systems, app stores, browsers, and search services.⁷⁴ Together these measures impose certain forward-looking duties on large platforms while remaining narrowly focused and leaving general enforcement to the Japan Fair Trade Commission under the Anti-Monopoly Act.

Content Regulation

Content governance is managed through a mix of consumer-protection statutes and sectoral oversight. Rather than a standalone “online harms” regime, Japan has opted for disclosure-based duties under its transparency laws, complemented by voluntary industry standards and guidelines. This lighter-touch approach seeks to balance speech protections with consumer safeguards, while maintaining flexibility for innovation.

Data Protection

Data protection and cybersecurity remain pillars of Japan’s approach. The Act on the Protection of Personal Information (APPI), first enacted in 2003 and substantially revised in 2017 and 2022, provides a comprehensive privacy framework, including consent and usage limits, breach notification, and strict penalties.⁷⁵ Japan has also deepened its digital identity regime through the My Number system, integrating health and welfare services into a single ID despite public concerns about glitches and privacy. Cybersecurity has been elevated with the Active Cyber Defense Law of 2025, which empowers authorities to take pre-emptive measures against cyber threats under defined oversight mechanisms.⁷⁶ Japan’s strategy also emphasises enabling digital adoption and innovation. The creation of the Digital Agency reflects efforts to modernise government IT, while METI’s “Mira-Digi” portal provides subsidies and advisory services to help SMEs accelerate digital transformation. Initiatives promoting cashless payments and e-government further underscore a state-driven digitalisation model.⁷⁷



South Korea

Competition Oversight

South Korea’s digital governance reflects both its highly connected society and attempts to provide opportunities across market participants. Competition oversight is led by the Korea Fair Trade Commission (KFTC), which has taken an active role in scrutinising platform conduct. Early proposals for a dedicated Platform Competition Promotion Act evolved into amendments to the existing competition law, equipping the KFTC with powers to address unfair practices such as self-preferencing, tying, and exclusivity. In parallel, the KFTC advanced the Online Platform Fairness Act to address platform-to-business (P2B) relationships. The draft would have introduced transparency and contractual fairness obligations on large platforms toward smaller business users, echoing elements of the EU’s P2B Regulation. However, the bill stalled amid concerns from industry and trade partners, and was ultimately not enacted. While the regime remains formally *ex post*, it is backed by strong investigatory capacity and selective *ex ante*-style obligations, such as Korea’s early adoption of app-store payment choice requirements.⁷⁸ Contestability concerns persist, however, with international firms noting that enforcement disproportionately affects U.S. platforms like Google and Apple, while major domestic players such as Naver and Kakao continue to dominate the super-app ecosystem.⁷⁹ The new KFTC chair nominee has indicated a desire to continue to pursue investigations using existing authorities, which is in contrast to indications by the Korean government that it would be suspending the push for a standalone comprehensive platform law in light of potential trade risks.⁸⁰

Content Regulation

Content governance is shaped through sectoral regulators and telecom frameworks. The Korea Communications Commission and the Ministry of Science and ICT oversee digital media, broadcasting, and online services, enforcing obligations on harmful content, online advertising, and platform liability. These powers are complemented by strong sectoral regimes in fintech and telecoms, giving regulators multiple levers to address online safety and consumer protection.

Data Protection

Data and digital rights are becoming a more prominent part of the policy mix. South Korea has developed a “bill of rights for data” to enhance portability and user control, aligning with its ambition to empower consumers and SMEs. Privacy protections under the Personal Information Protection Act (PIPA) provide a comprehensive regime, while the government continues to refine cybersecurity rules and promote ethical frameworks for artificial intelligence.⁸¹



Australia

Competition Oversight

Australia is shifting from case-by-case enforcement toward ex ante rules for the largest platforms. The ACCC's multi-year Digital Platform Services Inquiry (2017–2025) culminated on 23 June 2025 with recommendations for designated platform codes of conduct, an economy-wide unfair-trading prohibition, and stronger external dispute resolution. These proposals, while rooted in Australian law, functionally echo the EU's gatekeeper regime and reinforce the ACCC's conclusion that new regulatory tools are necessary.⁸² Canberra has also trialled muscular sectoral interventions: the 2021 News Media Bargaining Code compelled dozens of commercial agreements between platforms and publishers (including collective bargains by small outlets) that injected roughly AU\$200 million into Australian journalism in its first year. Together, these moves reflect an increasingly interventionist stance aimed at curbing entrenched market power without stifling competition.⁸³⁸⁴⁸⁵⁸⁶

Content Regulation

Australia has gone further on youth safety than anywhere else in the world. Parliament passed the Online Safety Amendment (Social Media Minimum Age) Act on 29 November 2024, requiring “age-restricted” social platforms to take reasonable steps to prevent under-16s from having accounts, with fines up to about AU\$49.5 million for non-compliance; enforcement begins on 10 December 2025 as eSafety issues detailed guidance.⁸⁷ Policymakers have described the package as world-first, and—unlike some overseas proposals—it does not include parental-consent carve-outs for under-16s.⁸⁸⁸⁹⁹⁰⁹¹

Data Protection

Privacy and portability are being modernised in tandem. Australia’s Consumer Data Right (CDR)—live for open banking from 1 July 2020 and expanded to energy on 15 November 2022—continues toward an economy-wide regime, with rules and assessments to extend into telecommunications and “open finance” (e.g., non-bank lending), so consumers can securely port their data across providers.⁹² In the wake of major breaches, the 2022 Enforcement Act lifted Privacy Act penalties and enhanced OAIC powers, and in late 2024 Parliament passed the Privacy and Other Legislation Amendment Act, strengthening individual rights, empowering the regulator, introducing a statutory tort for serious invasions of privacy, and establishing a Children’s Online Privacy Code—with further reforms flagged. The result is a GDPR-adjacent privacy framework paired with a uniquely Australian, standards-based portability regime—aimed at a safer, fairer digital ecosystem without derailing innovation.⁹³⁹⁴



The APEC snapshot highlights a patchwork of competition, content, and data rules, with some economies edging toward platform-focused measures and others relying on general frameworks. Against this backdrop, the EU’s Digital Markets Act (DMA) stands out as the most structured ex ante regime to date. Section 4 therefore examines the DMA in more detail, not as a prescriptive template but as a benchmark for assessing how APEC economies might adopt or adapt similar principles.



POLICY FOCUS: ADOPTION AND ADAPTATION OF DMA-INSPIRED POLICY IN APEC ECONOMIES



4.1 WHY FOCUS ON THE DMA?

The DMA is a useful reference point for this paper because it is the most fully articulated ex-ante, design-oriented regime for large platform intermediaries, even though its requirements are not yet tested and has had detractors even within the EU. Its obligations—non-discrimination in ranking, limits on tying and steering, interoperability and portability, user-choice defaults, and business-user data access—translate into engineering and product-design mandates enforced through regulatory supervision. Taking the DMA as a benchmark helps APEC policymakers evaluate what a similar approach would require in practice: continuous technical compliance work, measurable outcomes, and institutional capacity to audit complex systems rather than one-off case decisions. At the same time, as noted previously there is no global consensus that the DMA is the best approach and as noted further below implementing its provisions could create unintended consequences that mitigate or negate any benefits it provides. As such, APEC policymakers should not simply adopt the DMA as a model as this could actually chill investment and innovation, but rather study its impacts and decide which, if any, of its requirements make sense for an APEC context.

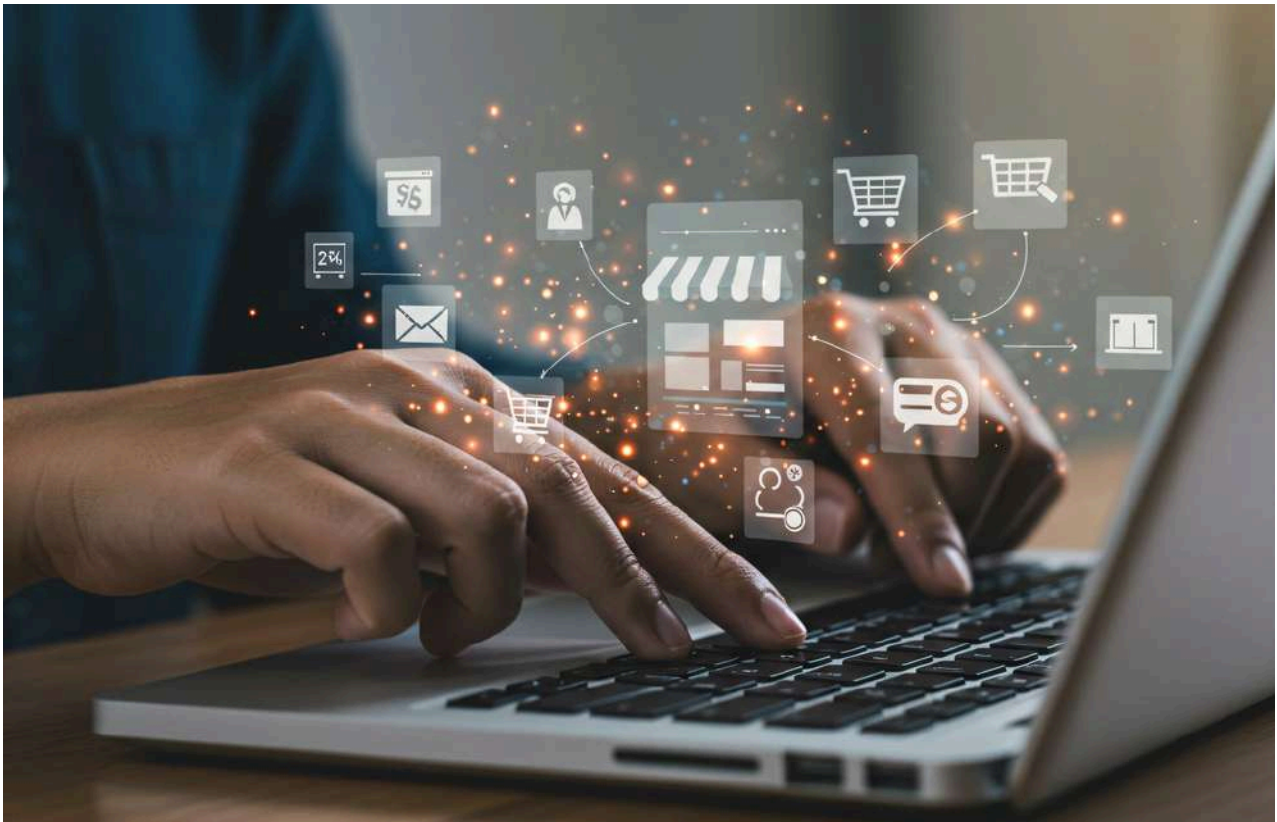


Pressure points targeted by the DMA, contestability in mobile ecosystems and app marketplaces, steering via payment rules, ranking neutrality, and access to data, do exist in APEC economies. But adopting DMA-style fixes raises non-trivial implementation questions. Anti-steering and default-choice obligations change the economics of distribution and payments and may produce pass-through or re-bundling elsewhere in the stack. Ranking neutrality is easy to state and hard to measure; it requires defensible metrics, access to logs, and clear standards for what counts as “undue” preference in complex, integrated interfaces. Data-access mandates interact with existing privacy rules, creating potential liability and governance gaps if consent, security, and onward-use controls are not specified up front. In short, the DMA’s mechanics imply a shift from principles to verifiable design, which in turn presupposes strong technical audit capability and clear guidance—features that vary across APEC authorities.

Global spillovers complicate the calculus. Gatekeepers often implement EU-driven changes worldwide for operational reasons, so DMA-shaped product decisions may arrive in APEC by default, irrespective of local law. That can import EU-specific compromises—new app distribution channels, alternative billing paths, choice screens, messaging interoperability—into markets whose safety baselines, consumer standards, and supervisory tooling were built around more centralized distribution. Where third-party channels expand, trust signals and age-gating may fragment unless baseline requirements for non-incumbent stores are articulated. Where interoperability is introduced, security boundaries and liability allocation need to be settled to avoid shifting risk to smaller services or end-users.

The focus of this analysis is on the DMA, because it is the instrument that acts directly on market structure, competition, and growth. By contrast, the DSA and GDPR function as guardrails: the DSA sets standards for safety and transparency, and the GDPR governs privacy and accountability. These frameworks matter, but only as background constraints within which competition policy operates.

4.2 IMPACTS OF THE DMA AND ITS IMPLEMENTATION TO DATE



One year into its enforcement, the Digital Markets Act (DMA) has rapidly shifted from rulemaking to active implementation. After designating seven "gatekeepers" by mid-2024, the European Commission set a March 2024 compliance deadline. Since then, regulators have aggressively monitored platform conduct, opening formal proceedings where they suspect violations and demonstrating a clear intent to enforce the new rulebook.

The Commission moved quickly, launching several high-profile investigations. Apple faced scrutiny for its App Store's "anti-steering" rules that prevent developers from informing users of cheaper purchasing options elsewhere. Google was investigated for self-preferencing its own services in search results and for its Play Store rules, while Meta's "consent or pay" subscription model was challenged for not offering users a genuine, free choice regarding data collection.⁹⁵⁹⁶ This culminated in the DMA's first fines in April 2025: a €500 million penalty for Apple over its anti-steering restrictions and a €200 million fine for Meta for its consent model.⁹⁷ The companies criticized the decisions for undermining privacy, security and choice as well as for discriminating against innovative U.S. technology companies and signalled their intent to appeal.⁹⁸

Beyond fines, the DMA has forced concrete changes in platform behaviour. Gatekeepers published compliance reports and began rolling out new features by early 2024. Apple committed to enabling alternative app stores and "sideloading" on iPhones in the EU.⁹⁹ Meta's WhatsApp started building the technical capacity for interoperability with other messaging services.¹⁰⁰ Google implemented a "choice screen" for search on Android and introduced new settings to prevent the combination of user data across its services.¹⁰¹

For MSMEs and developers, the DMA's first year brought both potential opportunities but also significant new hurdles. On one hand, the law introduced new rights, such as the ability to use alternative payment systems, access more platform data, and challenge unfair self-preferencing in search rankings. However, many benefits came with caveats. The anticipated wave of alternative app stores was modest and mostly limited to niche gaming sectors, leaving developers in other areas without meaningful new channels. Furthermore, opening up ecosystems created a "trust gap," making it harder for new apps outside official stores to persuade wary consumers of their safety.¹⁰²¹⁰³

Stakeholders like the European DIGITAL SME Alliance noted that compliance by gatekeepers often introduced new frictions, such as complex fee structures that dulled the benefits of new distribution options.¹⁰⁴ These fragmentation and compliance costs are felt more acutely by smaller firms, which must now navigate a more complex and shifting regulatory landscape instead of a single, unified channel.

A key unintended consequence involved platform safety. The DMA's requirement for Apple to allow third-party app stores in the EU led to the appearance of pornography apps on iPhones, which were previously banned under App Store rules.¹⁰⁵ This development highlighted a critical trade-off between fostering competition and maintaining the curated content moderation and safety standards of a closed ecosystem, offering an important lesson for other regulators.

For policymakers in the Asia-Pacific and beyond, the DMA's early implementation offers valuable lessons. It shows that ex-ante rules can prompt swift action, but the net impact on innovation and MSMEs is complex and not always positive. There have been some developments that could benefit MSMEs (more options, new fairness rules) though these have been accompanied by significant headaches (new fragmentation, safety trade-offs).



4.3 HOW DMA DIFFUSES INTO APEC ECONOMIES

The DMA's influence in the Asia-Pacific is evident, but its uptake varies across contexts. Emerging Regulatory Economies are proceeding more cautiously, emphasising foundational digital economy regulations and selective enforcement while monitoring how ex ante regimes perform elsewhere. Advanced Regulatory Economies, by contrast, have begun incorporating elements of DMA-style rules while recognising that adopting it wholesale would not be effective or appropriate, reflecting their stronger institutional capacity to oversee gatekeeper obligations and address structural concerns. The broader trajectory points to a trend toward greater attention to contestability and fairness, though jurisdictions differ significantly in how far and how quickly they move. In this sense, the DMA functions less as a wholesale model and more as a reference point for comparison, shaping debates over how digital platform regulation might evolve in the APEC economies.

Emerging Regulatory Economies



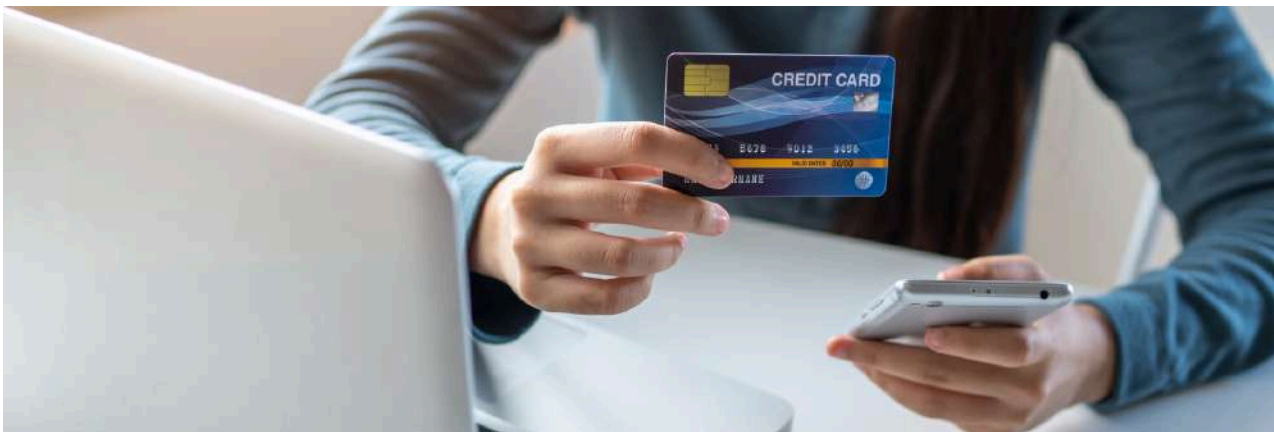
EREs generally have younger competition regimes and more nascent digital regulation, and they are taking a more incremental, adaptive approach to DMA-like policies. Rather than immediately codifying strict “dos and don’ts” for gatekeepers, many are embedding platform-accountability measures into refreshed consumer protection, e-commerce, and sectoral laws. Several ASEAN members have updated e-commerce rules and consumer codes to tighten online marketplace practices (truthful algorithms, transparent seller terms, basic consumer data protections), creating a fairness baseline without singling out gatekeepers. Vietnam and Indonesia, for example, now require online marketplaces to verify sellers and handle consumer complaints—raising accountability in practice even without a dedicated DMA-style law.¹⁰⁶¹⁰⁷ Parallel moves on data privacy and content (e.g., Thailand’s PDPA, Indonesia’s PDP Law) provide foundational guardrails on privacy, safety, and consumer rights before authorities waded into market-power rules.

On competition, ERE authorities are favouring ex post enforcement and cautious probes over sweeping new statutes. Some have opened antitrust investigations to test specific conduct theories, building an evidence base before writing ex ante codes. Indonesia’s KPPU has been active—beyond the Google Play billing case, it has examined exclusivity and discrimination issues—while Malaysia’s MyCC has run market studies in food delivery and ride-hailing, signalling readiness to intervene under the Competition Act if needed. The Philippines’ PCC has, by recent statements, held off from pushing a DMA-style regime, preferring to monitor markets and use existing tools. This “sit-and-learn” posture, echoed across EREs, reflects a pragmatic concern that importing rigid EU-style rules too quickly could raise compliance costs, chill investment, and, crucially, shift burdens onto small developers and merchants.¹⁰⁸

Approaches in the region remain cautious and calibrated. In Thailand, policymakers studied digital-competition needs since 2017 and tracked EU developments, but plans for a Platform Economy Act have been shelved, with regulators instead relying on existing instruments and targeted decrees. Indonesia has explicitly cited the EU DMA as a reference point for platform governance while stressing that direct transplantation would be ill-suited to domestic conditions. Both examples illustrate how emerging markets prefer to adapt gradually rather than lock in design mandates that may not fit their institutional or market realities.¹⁰⁹

In practice, EREs are leaning into “soft law” and co-regulation now, with potential for harder law later. ASEAN discussions around voluntary platform codes—commitments not to misuse data, to avoid self-preferencing, and to keep channels open for MSMEs—offer a low-friction path while capacity and evidence mature. Policymakers consistently frame interventions around MSME empowerment and digital inclusion rather than punitive “Big Tech” narratives. Notably, in Indonesia’s app-store remedy, KPPU emphasized harms to local developers and required fee reductions when alternative billing is used—a pro-MSME slant that mitigates pass-through costs. A realistic appreciation of capacity constraints keeps the focus on building tools, talent, and cross-border cooperation, so that any future ex ante rules are proportionate, technically workable, and do not unintentionally raise barriers for the smallest firms.¹¹⁰

Advanced Regulatory Economies



These countries are proactively formulating or implementing targeted conduct rules for digital “gatekeepers,” Though they differ in scope and approach. They tend to have relatively mature competition agencies and legal frameworks, which allow them to adapt the certain concepts from the DMA more directly.

For instance, as noted, Japan has passed a narrow law governing mobile OS, app stores, browsers and search services, addressing issues of default settings, self-preferencing, data use, and alternative access in those domains.¹¹¹ The Australian government, following a series of digital platform inquiries, proposed in late 2024 a new ex ante digital competition regime that closely mirrors the spirit of the DMA (with a public consultation on designating major platforms and imposing upfront rules on them). Australia is also considering mandatory codes of conduct enforced by its competition watchdog, covering platforms like app marketplaces and ad tech services, to ensure fair-play rules (a model akin to the DMA/UK approach).¹¹²

South Korea, another advanced player, became a pioneer by amending its Telecommunication Business Act in 2021 to ban app store operators from forcing the use of their own in-app payment systems – effectively an anti-monopoly design rule that aligns with DMA obligations on payment choice. Korea has been actively considering a broader “DMA-style” bill covering various gatekeeper practices, though that effort has faced significant pushback due to concerns that it discriminates against U.S. companies along with questioning of the premise that active competition does not already exist in the platform economy there. As the country continues to study the issue, it also continues to enforce platform competition via its existing laws including through the aforementioned active approach from the KFTC.¹¹³

Singapore, while not yet introducing a specific digital markets law, stands out for its proactive regulatory stance: the Competition and Consumer Commission of Singapore (CCCS) has conducted digital market studies, issued detailed guidelines on online platforms, and even established a dedicated *Data and Digital Markets unit* to build internal expertise. Singapore's strategy has been to lay the groundwork – in knowledge and soft regulation – for potential conduct rules, ensuring it can move quickly if intervention becomes necessary.¹¹⁴

These advanced regulatory economies also generally have higher enforcement capacity and clearer criteria for targeting big tech. They are defining thresholds (much like the EU's gatekeeper criteria) to know which companies would be subject to new rules. For example, Japan's law will use a Cabinet Order to designate which digital giants are covered, almost certainly singling out Apple and Google based on their market scale. Australia's proposal similarly discusses criteria for designation (revenue, user base, etc.), and Singapore's discussions often reference turnover or impact metrics to identify *substantial market power* in digital services. South Korea's proposed law has similarly set thresholds, though these appear designed to mainly target U.S. companies while carving out Korean and Chinese competitors.

Additionally, these regulators are delving into areas like transparency and interoperability pilots. Australia and Singapore have explored data portability and interoperability initiatives (Australia's Consumer Data Right, initially for banking, is expanding to other sectors and could intersect with platform data portability). Japan's law explicitly will require things like browser choice screens and data export tools to enhance user freedom.¹¹⁵ Even on mergers, these advanced jurisdictions are sharpening their scrutiny – for instance, Australian and Japanese authorities in recent years signalled they will closely review acquisitions by major platforms even if the targets are small (recognising the “killer acquisition” risk in digital markets).¹¹⁶



ANALYSIS: ASSESSING THE REGULATORY FIT FOR APEC ECONOMIES

Digital platforms have flourished across APEC economies under relatively light-touch rules, and what is working well today has been driven by market forces rather than heavy-handed regulation. Major platforms, both global and homegrown, have strong incentives to maintain user trust and therefore have voluntarily improved outcomes in areas like privacy, cybersecurity, accessibility, and intellectual property (IP) protection.

For example, leading tech firms have adopted stricter privacy controls and transparency features in response to public demand, even where local privacy laws are minimal. Likewise, e-commerce and content platforms have invested in cybersecurity defences and fraud prevention to protect their users, knowing that security lapses would damage their reputations. Accessibility features—such as multi-language support, assistive interfaces, and offline functionality—have expanded largely because companies see inclusive design as good business in diverse Asian markets. Even in IP enforcement, several marketplaces in the region now proactively remove counterfeit goods or pirated content through voluntary “notice-and-takedown” programs and partnerships with rights holders. All of this market-driven progress has occurred without prescriptive platform-specific regulation, suggesting that innovation and consumer expectations have steered platforms toward better practices organically.

However, as digital platforms become ever more central to APEC economies, policymakers face a set of core regulatory challenges. These challenges stem from the unique characteristics of platform markets and the need to balance multiple policy objectives. In attempting to address perceived problems regulators must be careful not to undermine the very dynamics that have spurred digital growth.



5.1 CHALLENGES

Competition and Algorithmic Fairness

A fundamental challenge is curbing anticompetitive behaviour, such as biased rankings of content, unfair self-preferencing of a platform’s own services, or steering users toward certain choices, without disrupting platforms’ own quality control. Many digital platforms currently police themselves to a degree: they refine algorithms to improve user experience and routinely de-rank low-quality or harmful content to keep their ecosystems trustworthy. For MSMEs, algorithmic transparency and fair treatment are critical: biased curation can push smaller sellers to the margins, while effective ranking systems can amplify their reach. Overly rigid rules could make platforms hesitant to tweak algorithms for fear of violating the law, even when those tweaks would benefit users or business partners. In APEC’s dynamic markets, where consumer preferences change rapidly, this could translate to stagnation or a one-size-fits-all ranking approach that serves neither users nor sellers well. Blanket bans on self-preferencing could also weaken integrated ecosystems that provide MSMEs with bundled logistics, payments, or mapping services that lower entry barriers. Poorly designed rules might thus hurt smaller firms more than the incumbents they aim to discipline.¹¹⁷

Data Access, Privacy, and Transparency

Closely tied to these competition concerns are questions of data access and transparency. MSMEs seek to comply with privacy laws and benefit from the consumer trust such compliance can generate. MSMEs also, however, benefit from better access to platform data—analytics on customer behaviour, search rankings, or ad performance—to improve their offerings and compete. For example, an MSME retailer in a regional e-commerce marketplace wants detailed analytics on how customers find and interact with their products.

As stronger privacy laws are adopted across APEC, in line with international frameworks such as the GDPR, to restrict data-sharing, tension is created between privacy, data access, and ease of compliance. If regulations mandate broad data access, privacy and compliance burdens may fall disproportionately on MSMEs, which lack the resources and compliance departments of larger firms to manage them. The challenge, therefore, is to enable useful transparency and data portability that can empower business partners and foster competition, without undermining privacy standards or violating the trust that users place in platforms. Initiatives such as the Global Cross-Border Privacy Rules (CBPR) Forum—adopted by many APEC economies including the United States, Korea, Japan, and Singapore—seek to strike this balance by promoting interoperable privacy frameworks that safeguard consumer trust while facilitating responsible data access for businesses.¹¹⁸ In short, policymakers must strike a balance: enabling practical, privacy-safe transparency tools that empower MSMEs without saddling them with compliance obligations they would struggle to meet.¹¹⁹

Bundling and Default Settings

These dilemmas also surface in debates over bundling and default settings. Bundling services and controlling default choices are central to platform competition debates, and in Asia-Pacific they carry particular weight given the widespread use of integrated digital ecosystems that combine transport, payments, shopping, and more. While regulators in Western markets worry that pre-loading apps like browsers or stores disadvantages rivals, in APEC contexts, bundling has often delivered real consumer benefits by lowering barriers and offering convenience where infrastructure is fragmented. The policy challenge is to prevent anti-competitive lock-in without dismantling models that have enabled millions of consumers and small businesses to access the digital economy. Rules that forbid pre-installation or force unbundling may level the playing field but risk reducing functionality or confusing less tech-savvy users. Striking the right balance requires distinguishing when bundling is exclusionary versus innovative, and grounding regulatory approaches in local consumer welfare outcomes rather than importing one-size-fits-all models.¹²⁰

Switching Costs and Interoperability

A related issue is the role of switching costs and interoperability in shaping competition. Reducing barriers to move between platforms—through measures like interoperability and data portability—is a common regulatory goal aimed at lowering switching costs that otherwise lock users and businesses into dominant services. High switching costs often disadvantage MSMEs more than consumers, since smaller businesses lack the capacity to manage multiple storefronts or marketing channels. Interoperability and portability rules could, in principle, help MSMEs by lowering dependence on a single platform. Yet mandating open systems creates technical and security challenges that smaller firms cannot easily navigate. One challenge is maintaining security and performance standards across interoperable services. For example, if a messaging platform in one APEC country is forced to interconnect with another global messaging service, differences in encryption protocols or safety features could expose vulnerabilities or degrade the user experience. If compliance obligations shift onto MSMEs—such as maintaining interoperable data formats or managing exports of customer records—the costs may outweigh the benefits.

Importantly, users and businesses in many APEC economies already demonstrate multi-homing behaviour, using multiple platforms for similar tasks when it suits them. This organic switching reduces lock-in and mitigates many of the concerns around high switching costs, suggesting that heavy-handed interoperability mandates may not be necessary. Regulators may therefore prioritise removing artificial switching barriers, such as restrictive contracts or proprietary APIs, while recognizing that user and business behaviour already provides a measure of contestability in platform markets.¹²¹

Limits of Regulatory Capacity

Finally, these challenges are compounded by limits in regulatory capacity across the region. APEC economies must not only decide what problems to regulate but also whether their agencies have the tools to enforce new mandates effectively. Advanced jurisdictions use complex criteria like “gatekeeper” or “core platform service,” tied to global revenue or user thresholds, but these can be vague or ill-suited to local markets while posing a risk to innovation. A threshold that captures systemic firms in large economies might misclassify smaller regional players or miss smaller firms with unique power in a certain category, while rapid shifts in business models create further ambiguity. This uncertainty complicates business planning and risks uneven enforcement. At the same time, many APEC regulators are still building the expertise and resources needed to monitor algorithms, enforce conduct rules, and resolve disputes. Experience elsewhere shows such oversight is resource-intensive, and in contexts where budgets and technical capacity vary, agencies may struggle to enforce broad mandates consistently. The challenge is thus twofold: to craft clear, context-appropriate definitions that do not discriminate and achieve clear policy objectives, and to ensure regulators have the tools and staff to implement rules effectively. Without this, even well-intentioned regulations risk faltering or creating more confusion than clarity.¹²²



5.2 COSTS

When regulatory models developed elsewhere are applied inaptly to APEC economies, they risk missing pro-competition or consumer goals while imposing collateral burdens that stifle innovation and inclusive growth. Unadapted rules can fragment markets, raise compliance costs, slow innovation, create new frictions for MSMEs, and harm consumers. Policymakers must weigh these risks carefully, as an imbalance could undermine the very enterprises and innovation such regulations aim to support.

Regulatory Fragmentation

One of the most immediate risks is regulatory fragmentation. APEC as a region thrives on cross-border digital trade and the scalability of tech business models across multiple economies, but divergent or poorly harmonized regulation threatens to splinter this integrated digital economy. In Europe, the DMA applies uniformly across the EU single market, preventing internal fragmentation. APEC economies, by contrast, regulate independently, so adopting DMA-style rules without coordination – aside from some of the potentially negative outcomes discussed previously – could amplify divergence rather than reduce it. A patchwork of definitions, requirements, and enforcement approaches forces platforms to create “parallel builds” for each jurisdiction, raising compliance and development costs while reducing interoperability. A tech firm might need to maintain one version of its app or service for Country A’s rules, another variant for Country B, and so on, fragmenting what could have been a single, scalable platform. This disproportionately burdens smaller firms and startups, which lack the resources to customize for multiple markets. In contrast, a large multinational platform can marshal compliance teams in each country, but even for them the lost economies of scale are significant. Over time, fragmentation could slow the spread of new digital services and undermine APEC’s long-standing goals of regional integration and digital trade facilitation.¹²³

Compliance Infrastructures and Barriers to Entry

Closely related to fragmentation are the heavy compliance infrastructures that sweeping platform rules require. Even one set of obligations can demand major fixed investments in engineering, legal oversight, and reporting systems, requiring firms to re-engineer core functions, document algorithmic changes, and maintain audit trails. While global tech giants may be able to absorb these costs, homegrown or mid-sized APEC firms face proportionately heavier burdens, diverting scarce capital and talent from growth. Over time, such fixed costs create barriers to entry and expansion, favouring incumbents and constraining startups and MSMEs who either struggle to meet the requirements or must contract their operations to avoid crossing regulatory thresholds. They can also slow innovation, as every new feature or experiment must clear layers of compliance checks. Thus, compliance build-out not only raises costs but risks dulling the innovative edge of regional firms in fast-moving digital markets.

Time-to-Market Delays

These compliance demands also feed directly into time-to-market delays, another significant cost of misfitted regulation. Digital innovation often depends on speed, but heavy rules can slow development cycles by diverting engineering and product teams to compliance projects instead of new features. Legally mandated redesigns or data tools typically take priority, forcing firms to postpone improvements that might benefit MSMEs or underserved users. In APEC's context, this delay may be felt most acutely in the rollout of features tailored for small businesses and underserved communities, because those are often on the "nice-to-have" list compared to legally necessary changes. Over time, these delays reduce platforms' responsiveness to user needs and dampen innovation across the ecosystem. For startups and smaller firms, even modest delays can be decisive, widening the gap with larger competitors that can spread compliance tasks across bigger teams. In this way, regulatory demands risk dragging down the pace of digital progress at a moment when APEC economies rely on rapid innovation to drive growth.¹²⁴

MSME Onboarding and Inclusive Growth Risks

The effects are especially acute for MSMEs at the point of entry. Ill-suited regulations can make it harder for small businesses to access digital platforms, which have been vital for levelling the playing field in APEC economies—allowing a micro-entrepreneur in a rural province to sell goods nationwide, or enabling a small startup to distribute its app without brick-and-mortar intermediaries. Stricter vetting, documentation, or compliance checks—such as paperwork to combat counterfeits or app reviews for content rules—can slow onboarding and add costs. Large firms can absorb these hurdles, but small businesses and indie developers may be discouraged or priced out. Over time, such frictions risk reducing MSME participation and undermining the inclusive growth that platforms have enabled across the region.¹²⁵

Consumer Welfare Trade-offs

Consumers too may face trade-offs if regulation overshoots its target. Rules that force unbundling or limit defaults can reduce convenience by requiring multiple apps or extra setup steps, while integrated features like payment wallets or unified logins may be curtailed. Rising compliance costs may also be passed on through higher fees or fewer free services, especially if platforms can no longer cross-subsidize offerings. In such cases, consumers may face higher prices or diminished choice—the opposite of what pro-competition regulation intends.¹²⁶

Taken together, these risks underline the stakes for APEC. The costs of an ill-fitted regulatory approach could manifest in fragmented markets, heavy operational burdens, slower innovation, higher entry barriers for MSMEs, and consumer welfare losses. These outcomes would undermine the goals of empowering innovation and inclusive growth that APEC economies prioritize. As such, any regulatory intervention in digital platforms must be proportionate and context sensitive. The analysis of challenges and costs above suggests that one-size-fits-all solutions from abroad do not cleanly fit APEC's diverse and dynamic digital landscape. A balanced path—learning from global

experiences (both positive and negative) but tailoring actions to local realities and weighing trade-offs carefully—will be essential to ensure regulation truly benefits competition, consumers, and innovation in the Asia-Pacific. In short, misaligned regulation risks fragmenting markets, raising costs, and slowing innovation—burdens that fall hardest on MSMEs. Since MSMEs account for over 98 percent of enterprises across APEC and are central to inclusive growth, policymakers must design rules proportionate to capacity and mindful of regional realities. A context-sensitive, proportionate approach is essential to ensure regulation empowers rather than constrains the smaller firms that drive competition and innovation.¹²⁷



5.3 QUANTIFYING THE COSTS

While qualitative assessment highlights the potential distortions of platform regulation, translating these into quantitative terms provides a clearer sense of scale and distributional impact. To do this, we follow a similar conceptual frame as the DMC Forum study *Economic Impact of the Digital Markets Act on European Businesses and the European Economy*: compliance costs are modelled as efficiency losses on the value of digital sales mediated by platforms, then aggregated across sectors and economies. Where the DMC Forum derived loss percentages from specific DMA provisions (e.g., consent rules, search neutrality), we adapt the approach to APEC by applying three illustrative scenarios—low (0.1%), medium (0.5%), and high (2%) of platform-mediated sales—reflecting varying levels of regulatory scope, fragmentation, and implementation burden.

The approach focuses on three core aspects: e-commerce, digital advertising, and app distribution. Together, these account for the majority of platform-mediated digital transactions and map directly onto areas targeted by ex-ante rules in regimes such as the EU's Digital Markets Act.



Data Sources

E-commerce GMV is drawn from regional and national sources. For EREs, the *Google–Temasek–Bain e-Economy SEA 2024* report provides estimates of gross merchandise value across consumer retail and services. For AREs, figures are taken from official statistics and industry reports, such as Japan's Ministry of Economy, Trade and Industry (METI) e-commerce survey, Statistics Korea's online shopping data, IMARC Group reports, and Singapore's Infocomm Media Development Authority (IMDA). To approximate the share mediated by platforms, we assume that 75 percent of e-commerce transactions occur via marketplaces rather than direct websites, a midpoint consistent with estimates that 70–80 percent of online retail in Southeast Asia flows through large marketplaces like Shopee, Lazada, and Tokopedia.^{128,129} Similar marketplace dominance has been documented in emerging Asia more broadly, where logistics, payments, and discovery advantages tilt activity toward platforms.¹³⁰



Digital advertising spend is taken from sources such as Dentsu’s annual advertising expenditure surveys, Statista market data, and IMARC country reports. This includes search, social, video, and display advertising. Based on industry breakdowns, we apply a platform share of 80 percent, reflecting the dominance of global intermediaries in search and social channels relative to independent publishers. Industry forecasts consistently place the combined share of search and social between 75 and 85 percent of digital ad spend across Asia-Pacific.¹³¹¹³²¹³³

App distribution is more difficult to measure consistently, but remains a critical part of the digital economy, especially in AREs such as Japan and Korea where gaming and app-based services are major revenue drivers. We draw on country-level estimates from Data.ai’s State of Mobile reports, Statista market data, and developer revenue surveys. For ERE economies, where granular country data are sparse, we use Southeast Asia regional totals from Data.ai and allocate proportionally by population and smartphone penetration. Given the highly intermediated nature of the app economy, we apply a platform share of 95 percent, reflecting that nearly all paid downloads and in-app purchases occur through the two dominant app stores (Apple App Store and Google Play).

Calculations and results

The results show that aggregate compliance costs are modest in macroeconomic terms but carry significant implications for market participants. In the medium scenario, ERE economies together face compliance costs of roughly USD 0.73 billion annually, while ARE economies face USD 2.34 billion. Combined, this amounts to just over USD 3 billion, or approximately 0.02 percent of the combined GDP of these nine economies. At this level, the aggregate impact may appear negligible. However, distribution matters: because small and medium-sized enterprises (SMEs) account for the majority of sellers, advertisers, and developers on these platforms, they absorb around 70 percent of the modeled burden. In ERE economies in particular, this translates into costs of USD 0.51 billion—small in national accounts, but material in the operating budgets of micro-enterprises and startups that depend on digital platforms as their primary route to market.

Group	Platform-Mediated Value (USD B)	Low (0.1%)	Medium (0.5%)	High (2%)	SME Share (≈70%) Medium
ERE (5 economies)	146.7	0.15B	0.73B	2.93B	0.51B
ARE (4 economies)	467.9	0.47B	2.34B	9.36B	1.64B
Total (APEC-9)	614.6	620M	3.07B	12.29B	2.15B

The scenarios also illustrate variation across countries. For Indonesia, the largest ERE digital economy, compliance costs under the medium scenario are estimated at USD 335 million, with MSMEs absorb roughly USD 234 million. In Thailand, total costs are around USD 129 million, of which MSMEs account for about USD 90 million. Vietnam faces a slightly lower burden at USD 87 million, with MSMEs carrying roughly USD 61 million. In Malaysia, compliance costs are estimated at USD 81 million, with MSMEs absorbing about USD 57 million, while in the Philippines the total reaches USD 102 million, of which MSMEs bear approximately USD 71 million.

Among ARE economies, Japan and Korea account for the largest absolute costs—USD 844 million and USD 732 million respectively—with MSMEs carrying an estimated USD 591 million and USD 512 million of those totals. Australia and Singapore face smaller nominal burdens, at around USD 228 million and USD 43 million respectively, but here too MSMEs bear the majority share, at approximately USD 160 million and USD 30 million. Relative to GDP, however, Korea shows the heaviest proportional impact, with compliance costs approaching 0.04 percent under the medium scenario.

At the high scenario, modelled at two percent of platform-mediated sales to reflect a fragmented DMA-like regime with heavier obligations, total costs rise to USD 12.3 billion across the nine economies. Even then, the macroeconomic share remains low, at just over one-tenth of one percent of combined GDP. But again, the distribution matters: MSMEs would carry an estimated USD 8.6 billion, a level that risks constraining their capacity to invest in growth, hire, and innovate. Using the DMA as a blueprint in the APEC context would mean replicating a more prescriptive and compliance-heavy regime—requirements for data access, interoperability, reporting, and auditing—that larger multinational platforms may be able to absorb, but which would impose disproportionate burdens on smaller firms. Such obligations would not only raise costs but could reduce their ability to compete on the very platforms meant to support their growth. In contrast, under the low scenario (0.1 percent), aggregate costs fall below USD 620 million across all nine economies, a burden that could potentially be absorbed with minimal distortion to larger companies but that would still be felt disproportionately by MSMEs. This could translate into tighter margins, reduced marketing budgets, or slower hiring, underscoring that smaller firms are disproportionately sensitive to compliance costs at any scale.

Taken together, these results suggest that the regulatory “fit” question in APEC should be understood less in terms of aggregate GDP impact and more about the distribution of compliance costs. The same compliance architecture that may be absorbed by multinational platforms can impose disproportionate frictions on MSMEs that rely on those platforms for discovery, customer acquisition, and payments. In Emerging Regulatory Economies, where MSMEs dominate commerce and institutional capacity is lower, the risks of miscalibration are therefore more acute. Advanced Regulatory Economies, by contrast, may absorb compliance more smoothly, though the modelled figures indicate that even there, costs cluster in highly digital sectors and fall disproportionately on smaller firms.



POLICY RECOMMENDATIONS — PATHWAYS TO SMART PLATFORM REGULATION

The recommendations below outline guiding principles, steps for domestic policy sequencing, avenues for regional coordination, and mechanisms for review. They are grounded in the recognition that digital platforms in APEC economies have flourished under light-touch regulatory approaches, generating significant benefits for consumers, MSMEs, and innovation. This experience underscores that regulation should not be pursued for its own sake. Instead, governments should carefully assess whether intervention is truly needed in a given area, and where appropriate, design proportionate measures that address specific risks without undermining the conditions that have enabled dynamic digital growth. The approach set out here seeks to achieve effective oversight of major online platforms in a way that supports innovation and competition, reflects regional contexts, and avoids unintended consequences.



6.1 GUIDING PRINCIPLES:

APEC policymakers should ground their platform governance efforts in several key principles to ensure regulations are *smart* – i.e. evidence-based, proportionate, and forward-looking:

Observe and Learn

Resist rushing into DMA-style legislation wholesale, as well as even in narrower areas until its real-world impacts are clearer. The EU has been a first mover with the DMA, but its effectiveness in boosting competition and innovation “remains to be seen” and has had detractors even within the EU. APEC economies will benefit from closely observing Europe’s rollout of obligations on Big Tech over the next couple of years – including any market responses, compliance challenges, and unintended side-effects. By building on lessons learned (both successes and shortcomings), regulators can design improved rules calibrated to local realities as appropriate and necessary.

Proportionality

Obligations should be proportional to the magnitude of harms addressed, while ensuring that those same obligations spare startups and smaller players from undue costs. Setting arbitrary thresholds based on revenue or user counts like the EU’s DMA, for instance, risks conflating size with market power, and could unintentionally create an unlevel playing field that actually exacerbates anti-competitive behaviours. Proportionality also means balancing new rules with privacy, cybersecurity, and IP protection, while allowing for data-sharing and interoperability between markets. Tailoring requirements in this way allows regulators to address harm effectively without overreach.

Inclusiveness

Regulatory development should be highly inclusive, with structured consultation involving platforms, MSMEs, app developers, consumers, and other stakeholders who will be directly affected. Early engagement through consultations, advisory councils, or industry roundtables helps surface practical concerns and refine proposals. South Korea’s draft “Online Platform Competition” law shows the risks of failing to build consensus. APEC economies should avoid such outcomes by making policy design collaborative—ensuring rules curb unfair practices without creating unfair compliance burdens or new barriers for smaller players, and incorporating user perspectives on privacy, choice, and fairness. An inclusive, multi-stakeholder process will yield more balanced, workable rules and greater trust in the regulatory regime.

Flexibility

Given the dynamism of digital markets, APEC regulators should prioritise flexible, innovation-friendly tools over rigid, one-size-fits-all prescriptions. Approaches such as pilot programs, phased rollouts, and regulatory sandboxes allow new compliance solutions or business models to be tested before rules are scaled up. For instance, an interoperability mandate could begin as a limited pilot between willing platforms to gather technical feedback, while phased rollouts give firms time to adapt and regulators time to refine. Safe harbours can also encourage proactive compliance, offering lighter oversight or delayed enforcement to platforms that exceed baseline standards. Overall, a flexible approach that adapts to technological change and diverse market conditions will mitigate risks of stifling innovation while still improving user safeguards—consistent with APEC’s emphasis on balanced, innovation-supportive regulation.

Coherence

Policymakers should ensure coordination across competition, consumer protection, privacy, and online safety, since platform issues cut across traditional regulatory silos. A single practice—such as self-preferencing by a dominant app store—can raise concerns in multiple domains, and if agencies act in isolation the result may be duplicative burdens or gaps. The EU’s experience shows how multiple regimes (DMA, DSA, GDPR) can create overlaps and contradictions, whereas APEC economies have the chance to design more coherent frameworks from the outset. Aligning definitions, avoiding duplication, and using inter-agency working groups can help ensure that rules on competition, privacy, cybersecurity, and consumer protection reinforce rather than conflict with one another. A coherent approach will simplify compliance, strengthen enforcement, and more effectively govern digital markets.



Regional Compatibility

APEC economies should pursue a degree of compatibility in platform regulations to reduce fragmentation and support cross-border digital trade. While full harmonization is unlikely, baseline alignment on key issues would lower compliance costs and give businesses, especially MSMEs, clearer rules across markets. Cooperation can also ensure that competition and privacy regimes complement one another regionally, drawing on principles of mutual recognition. By adapting positive aspects of regulatory regimes outside the region while respecting local diversity, APEC can create interoperable, forward-looking frameworks that balance alignment with flexibility.



6.2 DOMESTIC POLICY SEQUENCING

Translating these principles into action requires careful sequencing. Rather than leaping into comprehensive DMA-style laws, APEC economies should choose lighter tools, build capacity, and expand only as evidence and readiness grow. In practice, this means applying the guiding principles outlined in Section 6.1 as benchmarks for phasing and calibrating new rules.

Sequence Regulation Gradually

The uncertainties around DMA's outcomes – Will it truly spur more competition? What compliance challenges will emerge? – suggest that copying it wholesale would not be prudent for APEC economies. Instead, regulators can deploy narrower measures—such as standard transparency templates for app stores or marketplaces—to nudge better behaviour without legal mandates. Grace periods can ease adjustment when new rules are introduced, especially for smaller operators, while regulatory sandboxes allow platforms to pilot data portability or algorithmic transparency under oversight. In a sandbox, companies experiment with compliance solutions or new features under regulatory oversight and with legal flexibility. For instance, a few large platforms could enter a sandbox to pilot data portability features or algorithmic transparency mechanisms. Regulators would monitor outcomes, which inform better rulemaking later. These “test and learn” approaches generate evidence and feedback, laying the groundwork for more durable regulation later.

Articulate Outcomes

Guided by proportionality, regulators should articulate outcome-based principles—such as non-discrimination toward business users or easy data portability—that set objectives without dictating technical methods. Australia's approach to some emerging tech regulations, for instance, has emphasized performance-based guidelines over rigid rules, allowing for flexibility, encouraging creative compliance in fast-changing markets. An outcome-based code of conduct, published early by competition or telecom authorities, could signal acceptable practices and moderate behaviour even before binding law, while giving regulators a compass for enforcement if harms emerge.

Prioritize MSME enablement

Initial policy actions should focus on strengthening the environment for MSMEs—who make up over 98% of enterprises and 40–60% of GDP in most APEC economies—while equipping regulators with the right tools. MSMEs benefit from curbing exploitative practices but can be harmed if rules are too complex or costly. Governments should therefore empower and educate MSMEs through measures like public-private partnerships, helpdesks or ombudsman offices to resolve platform disputes, training programs and portals to explain rights and regulatory changes, and simple compliance templates to reduce legal burdens. These steps ensure MSMEs can seize the benefits of pro-competitive measures and prepare regulators to enforce them effectively.

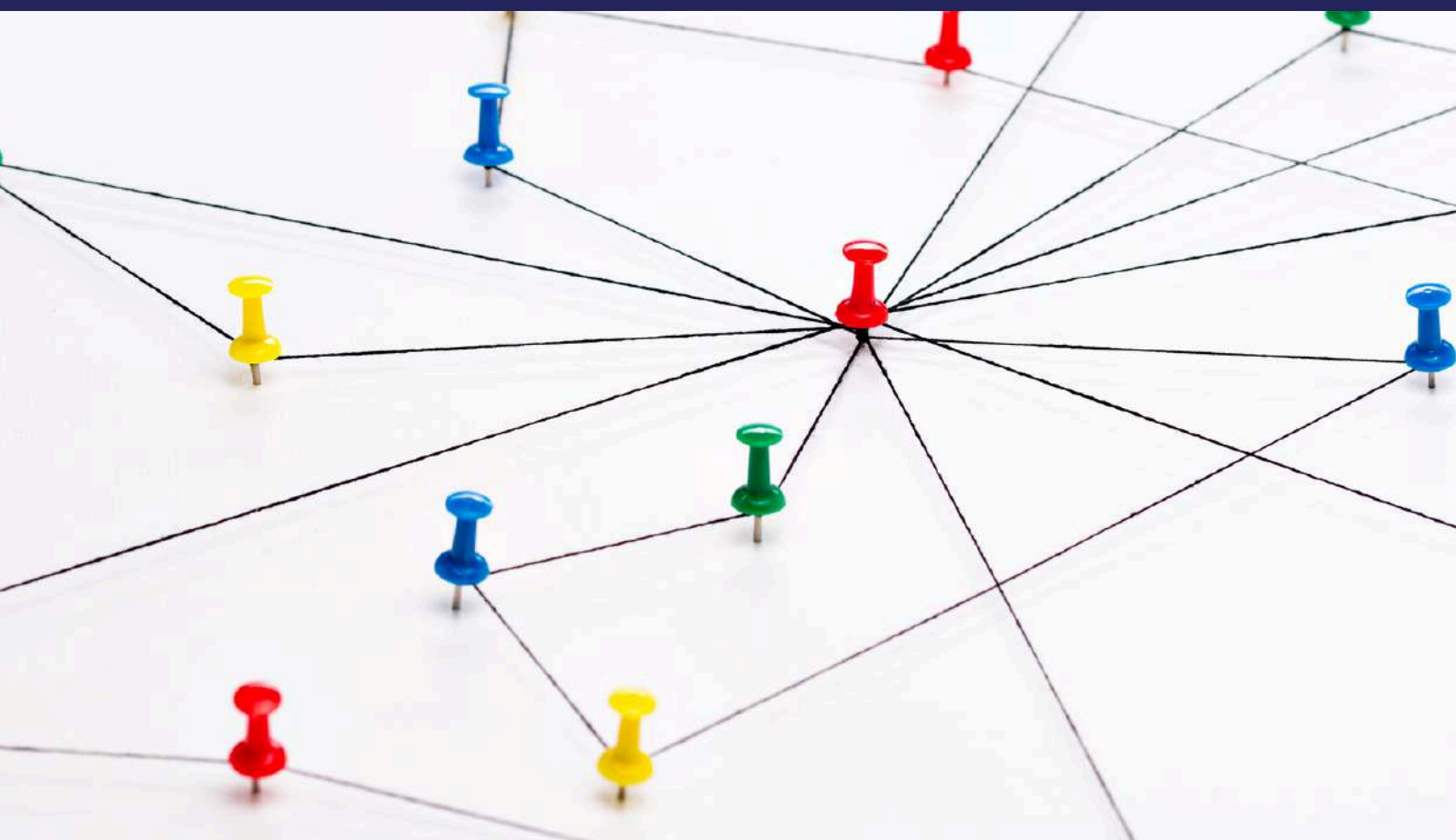
Build Regulator Capacity

To effectively oversee these complicated issues, regulators must first invest in personnel (data scientists, engineers, economists), upgrade technical infrastructure, and develop frameworks suited to multisided markets. Experts stress that intervention in fast-moving digital sectors requires deep technical and business understanding, and agencies like Singapore’s CCCS have already begun capacity-building through dedicated digital units and digital forensics training. By bolstering MSME support systems and regulatory expertise upfront, APEC economies lay the groundwork before trying to enforce obligations.



Calibrate by Country Context

APEC economies vary widely in regulatory maturity, so a one-size regulatory approach will not fit all. Advanced jurisdictions with well-resourced agencies—such as Japan, which in 2024 enacted a targeted law on smartphone app stores, and Australia, which is moving toward a new digital competition regime—can pilot robust measures and provide examples for the region to study. Emerging economies, by contrast, may benefit more from incremental steps, focusing first on connectivity, inclusion, and voluntary good practices where competition remains vibrant. Sequencing reforms this way avoid both extremes: neither overshooting with ill-suited rules nor lagging behind entirely. Regular APEC information-sharing can ensure later movers learn from pioneers, while pioneers adjust through peer feedback. In short, adopt a calibrated, multi-speed approach toward the common goal of fair and competitive digital markets.



6.3 REGIONAL AND INTERNATIONAL COORDINATION

Effective platform regulation cannot happen in isolation. Given the borderless nature of digital services, APEC economies should collaborate to create a more seamless regulatory environment across the region. Cooperation will help prevent regulatory arbitrage and reduce duplicative burdens on businesses, while still allowing local flexibility. There are several layers to this coordination:

Align Core Concepts and Standards

APEC members should work toward a shared framework of core definitions, principles, and procedural standards for platform regulation. This doesn't mean identical laws, but rather a common vocabulary and minimal standards that everyone recognizes. This alignment could be achieved through an APEC *Digital Platform Governance Principles* document or annex to a Ministerial Statement, wherein members endorse shared definitions. Such consistency would make it easier to coordinate enforcement actions and for businesses to know where lines are drawn.

Ensure Procedural Interoperability

Regulators could coordinate on due process standards – for instance, agreeing that platforms should respond to business user complaints or appeals within a certain timeframe (a service-level agreement, or SLA, for disputes). APEC might also identify “core ad transparency fields” for digital advertising and recommender systems (e.g. why an ad was shown, who paid for it, performance metrics, political targeting), ensuring comparable disclosures region-wide. Interoperable templates and data formats, like standardized transparency reports or common API formats for data portability, would further reduce compliance complexity. APEC’s Digital Economy Steering Group could lead by developing model guidelines or voluntary codes that economies can reference domestically. Done through consultation with industry and stakeholders, such alignment would deliver regulatory coherence while remaining practical and adaptive to technological change, limiting fragmentation and easing compliance across diverse markets.

Use Soft-Law and Mutual Recognition

Beyond formal alignment, APEC can draw on its tradition of non-binding cooperation to promote best practices through guidance notes or frameworks on issues like app store fairness or algorithmic transparency. Economies could voluntarily adopt these guidelines, creating de facto harmonization—much like the APEC Privacy Framework and its Cross-Border Privacy Rules (CBPR) system, which sets baseline standards recognized across borders. A similar approach for platform governance could include mutual recognition of compliance certifications: if a platform is audited in one economy against agreed APEC standards, others could accept that certification. This would reduce redundant audits, lower costs, and incentivize companies to meet high standards that carry region-wide credibility.

Draw on Existing Instruments

Economies can draw on tools like the APEC Model Contractual Clauses for data transfers when designing platform data-sharing or business-user rules, ensuring consistency with regional privacy norms. Aligning portability or access obligations with these clauses would prevent conflicts across jurisdictions. Building a structured network for digital market regulators to share information would enhance efficiency and coherence across the region.

Anchor Cooperation in APEC Forums

Regional efforts will likely take shape through Ministerial Meetings or Leaders’ Declarations, which can set political direction. An APEC Digital Ministers’ Declaration could, for example, outline shared principles and call for a toolkit or playbook on platform regulation, with Action Plans tasking sub-groups to develop technical standards like interoperable reporting formats. Anchoring cooperation in high-level statements helps sustain commitment while allowing economies to tailor specifics. As one APEC official noted, the forum’s value lies in “shared learning and joint action... building alignment where possible and respecting diversity where needed.”¹³⁴ Such coordination can drive convergence on foundational elements of platform rules, reduce fragmentation, and create a more predictable environment for platforms and the businesses that rely on them.



6.4 REVIEW & ADJUST

No regulatory framework for digital platforms should be static. Given the pace of technological change and evolving platform behaviour, APEC economies must embed a review-and-adjust mechanism to ensure policies remain proportionate and effective over time.

Continuous Monitoring of Key Indicators

Once initial measures are in place—whether soft tools, codes of conduct, or binding rules—regulators should track whether they achieve intended outcomes. A monitoring framework can combine stakeholder feedback with quantitative metrics such as:

- **Time-to-feature rollout:** How quickly platforms implement required pro-competitive features, signalling either compliance challenges or regulatory feasibility.
- **MSME onboarding costs and time:** Whether MSMEs can more easily list apps or sell on marketplaces, measured through surveys and participation rates.
- **Appeal and dispute outcomes:** The volume, timeliness, and resolution of MSME or developer complaints, showing whether due-process reforms are effective.
- **Interoperability and data portability pilots:** Uptake, quality, and security outcomes of cross-platform trials, indicating whether mandates should be expanded or refined.
- **Cross-border compliance burden:** Costs for firms operating across APEC, highlighting whether regional alignment is reducing fragmentation.

Collecting and publishing such data—potentially through an annual APEC “state of digital markets” report—not only creates accountability but also encourages platforms to improve pre-emptively.

Formal Periodic Reviews

Building on monitoring, economies should schedule structured evaluations at regular intervals. Reviews should ask whether rules are fostering competition, fairness, and consumer choice; identify unintended consequences; and highlight new issues requiring attention.

Where evidence shows obligations are working—for example, data access rules boosting third-party services without harming privacy—regulators may expand them. Where rules prove overbroad or counterproductive—such as bans inadvertently restricting consumer-friendly integrations—they should be refined or suspended. Reviews should also remain transparent, with clear explanations to maintain credibility and collective learning across APEC.

Conclusion

Embedding review and recalibration makes platform regulation a process of continuous improvement rather than a fixed statute. By monitoring outcomes, holding evidence-based reviews, and sharing findings across the region, APEC economies can ensure their regulatory frameworks stay agile—scaling up what works, discarding what does not, and adapting to emerging technologies. This iterative model will sustain competition and innovation while protecting consumers, offering a pragmatic path that other regions may come to emulate.

BIBLIOGRAPHY

- ¹APEC. Statement of the Chair of the 28th APEC SME Ministerial Meeting. 2022. Singapore: APEC.
- ²APEC. Small and Medium Enterprises Working Group (SMEWG) Webpage. Accessed 2025. <https://www.apec.org>.
- ³Indonesia Ministry of Cooperatives and SMEs. Report on APEC Policy Dialogue on MSMEs. Jakarta: Ministry of Cooperatives and SMEs, 2024.
- ⁴United Nations, Department of Economic and Social Affairs, Population Division. World Population Prospects 2022. New York: United Nations, 2022.
- ⁵Google, Temasek, and Bain & Company. e-Conomy SEA 2023 Report. 2023.
- ⁶DataReportal. Digital 2024: Global Overview Report. January 2024.
- ⁷Information Technology and Innovation Foundation (ITIF). How Digital Services Empower SMEs and Start-Ups. Washington, DC: ITIF, August 27, 2025. <https://itif.org/publications/2025/08/27/how-digital-services-empower-smes-and-start-ups/>.
- ⁸Google, Temasek, and Bain & Company. (2023). e-Conomy SEA 2023 Report.
- ⁹Asian Development Bank (ADB). Asia Small and Medium-Sized Enterprise Monitor 2023. Manila: ADB, 2023.
- ¹⁰Organisation for Economic Co-operation and Development (OECD). OECD Digital Economy Outlook 2023. Paris: OECD, 2023.
- ¹¹Asia-Pacific Economic Cooperation (APEC). APEC Internet and Digital Economy Roadmap. Singapore: APEC Secretariat, 2022.
- ¹²Australian Competition and Consumer Commission (ACCC). Digital Platform Services Inquiry: Sixth Interim Report. Canberra: ACCC, 2023.
- ¹³Ministry of Trade and Industry Singapore. "Digital Economy Agreements." <https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements>.
- ¹⁴Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC). Model Artificial Intelligence Governance Framework: Second Edition. Singapore: IMDA and PDPC, 2020.
- ¹⁵Japan. Act on the Protection of Personal Information (Act No. 57 of 2003), as amended.
- ¹⁶Digital Agency (Japan). "Social Security and Tax Number System." <https://www.digital.go.jp/policies/mynumber>.
- ¹⁷Japan. Amendment to the Telecommunications Business Act, 2021.
- ¹⁸GSMA. The Mobile Economy Asia Pacific 2023. London: GSMA, 2023.
- ¹⁹Australian Government. "Consumer Data Right." <https://www.cdr.gov.au>.
- ²⁰Australian Competition and Consumer Commission (ACCC). Digital Platform Services Inquiry. Reports, 2020–2025. <https://www.accc.gov.au>.
- ²¹European Commission. "The Digital Markets Act: Ensuring Fair and Open Digital Markets." 2023. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.
- ²²European Union. Regulation (EU) 2022/1925 on Contestable and Fair Markets in the Digital Sector (Digital Markets Act), September 14, 2022.
- ²³Ibid., Article 2(2).
- ²⁴European Commission. "Commission Designates Six Gatekeepers Under the Digital Markets Act." Press Release, September 6, 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328.
- ²⁵Regulation (EU) 2022/1925, Articles 5, 6, and 7.
- ²⁶Ibid., Article 5(2) on combining personal data; Article 6(9) on data portability; Article 6(10) on access to data for business users; Article 14 on the obligation to inform about concentrations.
- ²⁷Ibid., Article 30.
- ²⁸Ibid., Article 18.
- ²⁹Bradford, Anu. The Brussels Effect: How the European Union Rules the World. Oxford: Oxford University Press, 2020.
- ³⁰European Commission. The Digital Services Act. 2023. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>.

- ³¹European Union. Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act), October 19, 2022.
- ³²European Commission. “Supervision of the Designated Very Large Online Platforms and Search Engines Under the DSA.” 2023. <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>.
- ³³Regulation (EU) 2022/2065, Chapter III, Sections 1–4.
- ³⁴*Ibid.*, Chapter III, Section 5 (Articles 34–48).
- ³⁵*Ibid.*, Article 52(3) for fines and Article 56(1) for periodic penalty payments.
- ³⁶European Commission, “Data Protection in the EU,” accessed August 14, 2025, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en.
- ³⁷Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 3.
- ³⁸*Ibid.*, Article 5 (Principles relating to processing of personal data) and Article 6 (Lawfulness of processing).
- ³⁹*Ibid.*, Chapter III (Articles 12–23)
- ⁴⁰*Ibid.*, Article 35.
- ⁴¹*Ibid.*, Article 37 (Designation of the data protection officer), Article 33 (Notification of a personal data breach to the supervisory authority), and Chapter V (Transfers of personal data to third countries or international organisations).
- ⁴²*Ibid.*, Article 83 (General conditions for imposing administrative fines).
- ⁴³Online Safety Act 2023, c. 30 (UK), received Royal Assent 26 October 2023. Full text available via UK Parliament legislation database. See also Ofcom, “Preparing for the Online Safety Act,” accessed August 14, 2025.
- ⁴⁴Digital Markets, Competition and Consumers Act 2024, c. 25 (UK), received Royal Assent 24 May 2024.
- ⁴⁵*Ibid.*, Part 1, Chapter 2 (Designation of undertakings with strategic market status) and Chapter 3 (Conduct requirements).
- ⁴⁶Clifford Chance, “A New Digital Regulatory Landscape: The UK’s Digital Markets, Competition and Consumers Bill,” April 26, 2023.
- ⁴⁷U.S. competition law is primarily addressed under the Sherman Antitrust Act of 1890 and the Clayton Antitrust Act of 1914. Copyright-related content takedowns are governed by the “safe harbor” provisions of the Digital Millennium Copyright Act (DMCA) of 1998.
- ⁴⁸Notable examples of state-level regulation include the California Consumer Privacy Act (CCPA) of 2018, which created new data privacy rights, and laws in states like Texas and Florida aimed at regulating social media content moderation.
- ⁴⁹Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*.
- ⁵⁰Congressional Research Service. Section 230: An Overview. Washington, DC: CRS, 2023.
- ⁵¹Cybersecurity Law of the People’s Republic of China. Effective June 1, 2017.
- ⁵²Data Security Law of the People’s Republic of China. Effective September 1, 2021.
- ⁵³Provisions on the Governance of the Online Information Content Ecosystem. Issued by the Cyberspace Administration of China, effective March 1, 2020.
- ⁵⁴Anti-Monopoly Law of the People’s Republic of China. Amended with effect from August 1, 2022. Application to the digital sector clarified in State Administration for Market Regulation (SAMR). Guidelines on Anti-Monopoly in the Field of Platform Economy. Beijing: SAMR, 2021.
- ⁵⁵Cyberspace Administration of China (CAC). China Internet Development Report 2024. Beijing: CAC, 2024.
- ⁵⁶Komisi Pengawas Persaingan Usaha (KPPU), Decision on the Acquisition of PT Tokopedia by TikTok Pte. Ltd. (2025); President of the Republic of Indonesia, Presidential Regulation No. 32 of 2024 on the Responsibility of Digital Platform Companies to Support Quality Journalism.
- ⁵⁷Indonesia, Ministry of Communication and Information Technology (Kominfo), Regulation No. 5 of 2020 on Private Electronic System Operators (PSE); Law No. 1 of 2024 (Second Amendment to the Electronic Information and Transactions Law, Law No. 11 of 2008).
- ⁵⁸Law No. 27 of 2022 on Personal Data Protection (PDP Law), enforceable from October 2024; Minister of Trade Regulation No. 31 of 2023 on e-commerce, prohibiting social media platforms from facilitating in-app transactions and setting a US\$100 minimum for cross-border sales.

- ⁵⁹Malaysian Communications and Multimedia Commission (MCMC), Determination on Licensing Framework for Online Application Services (2024); Malaysia Competition Commission (MyCC), Annual Plan 2025.
- ⁶⁰Communications and Multimedia (Amendment) Act 2025 (Malaysia); Malaysian Media Council Act 2025.
- ⁶¹Personal Data Protection (Amendment) Act 2024 (Malaysia).
- ⁶²Thailand, Royal Decree on the Supervision of Digital Platform Services Subject to Prior Notification, B.E. 2565 (2022), in force August 2023.
- ⁶³Trade Competition Commission of Thailand (TCCT), Draft Guideline on Unfair Trade Practices for E-commerce Platforms (2025); Electronic Transactions Development Agency (ETDA), Notification on Rules and Procedures for High-Risk Digital Platform Service Operators (2025).
- ⁶⁴Thailand, Personal Data Protection Act (PDPA), B.E. 2562 (2019); enforcement decisions published by the Office of the Personal Data Protection Committee (PDPC), 2025.
- ⁶⁵Philippine Competition Commission (PCC), Market Study on E-commerce and Online Advertising (2024); PCC, Guidelines on Motu Proprio Review of Mergers and Acquisitions in the Digital Economy (2023).
- ⁶⁶Republic of the Philippines, Republic Act No. 11967 (Internet Transactions Act of 2023).
- ⁶⁷*Ibid.*, plus Republic Act No. 10175 (Cybercrime Prevention Act of 2012); Republic Act No. 11479 (Anti-Terrorism Act of 2020); Republic Act No. 10173 (Data Privacy Act of 2012); and Republic Act No. 11934 (Subscriber Identity Module [SIM] Registration Act).
- ⁶⁸Socialist Republic of Vietnam, Law No. 20/2023/QH15 on Electronic Transactions (2023, with 2024 Decree); Law No. 19/2023/QH15 on Protection of Consumers' Rights; Law No. 23/2018/QH14 on Competition.
- ⁶⁹*Ibid.*, Decree Amending and Supplementing a Number of Articles of Decree No. 72/2013/ND-CP, effective December 2024.
- ⁷⁰*Ibid.*, Decree No. 13/2023/ND-CP on Protection of Personal Data; Law on Cybersecurity (2018) and Decree No. 53/2022/ND-CP; Law on Data (2025); and amended tax rules under Circular No. 80/2021/TT-BTC and the Law on Tax Administration (2025).
- ⁷¹Competition and Consumer Commission of Singapore (CCCS), Market Study on E-commerce Platforms (2020).
- ⁷²Republic of Singapore, Protection from Online Falsehoods and Manipulation Act 2019; Online Safety (Miscellaneous Amendments) Act 2022; Infocomm Media Development Authority (IMDA), Code of Practice for Online Safety.
- ⁷³Republic of Singapore, Personal Data Protection Act 2012; Ministry of Trade and Industry, Digital Economy Agreements; IMDA & PDPC, Model Artificial Intelligence Governance Framework, 2nd ed. (2020).
- ⁷⁴Japan, Act on Improving Transparency and Fairness of Digital Platforms (2021); Act on Promotion of Competition for Specified Smartphone Software (2024).
- ⁷⁵Japan, Act on the Protection of Personal Information (Act No. 57 of 2003), as amended (notably 2017 and 2022).
- ⁷⁶Japan, Act on the Establishment of the Digital Agency (2021); Act to Promote the Security of Our Nation and People through Integrated Economic Measures (2025).
- ⁷⁷Government of Japan, Digital Agency (digital.go.jp); Ministry of Economy, Trade and Industry, Mira-Digi Portal (miradigi.go.jp).
- ⁷⁸Republic of Korea, Telecommunications Business Act (Amendment 2021).
- ⁷⁹Y. Lee, "South Korea's Proposed Platform Law Hits a Snag," Lawfare, 2024.
- ⁸⁰Min-hyung Lee, "FTC to suspend push to regulate US platform firms amid trade risk," The Korea Times, August 14, 2025, ³⁴European Commission, "Data protection in the EU," European Commission, Accessed August 14, 2025. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en.
- ⁸¹Republic of Korea, Personal Information Protection Act (PIPA), last amended 2023.
- ⁸²Australian Competition & Consumer Commission (ACCC), Digital Platform Services Inquiry – Final Report (March 2025).
- ⁸³*Ibid.*: "Regulatory Reform in Digital Platform Markets Is Needed to Improve Competition and Consumer Outcomes," ACCC, 2025.
- ⁸⁴"Meta Is Ending Its Deals to Pay for Australian News Content. This Is How It Could Change Your Facebook and Instagram Feeds," ABC News, 2025.
- ⁸⁵"Australia's News Media Bargaining Code Pries \$140 Million from Google and Facebook," Poynter, 2022.

- ⁸⁶The Treasury, Australian Government. (2022). News Media and Digital Platforms Mandatory Bargaining Code - Review.
- ⁸⁷Australia, Online Safety Amendment (Social Media Minimum Age) Act 2024; enforcement details from eSafety Commissioner.
- ⁸⁸"Australia Passes Social Media Ban for Children Under 16," Reuters, November 28, 2024
- ⁸⁹"Australia Passes Social Media Platform Age Restriction Law," Pinsent Masons Out-Law.
- ⁹⁰"Families Battle Tech Giants as Australia Pushes for an Under-16s Social Media Ban," Wall Street Journal, 2024.
- ⁹¹Australia, Online Safety Amendment (Social Media Minimum Age) Act 2024. Enforcement details are provided by the eSafety Commissioner.
- ⁹²Dentons. "Australia's Data Portability Rights: An Update on What's Happening on the Consumer Data Right after Meagre Cost/Benefit Outcomes Come to Light." 2024.
- ⁹³Australia, Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022; Privacy and Other Legislation Amendment Act 2024; Consumer Data Right (CDR), administered at cdr.gov.au.
- ⁹⁴Norton Rose Fulbright, "Australian Privacy Alert: Parliament Passes Major and Meaningful Privacy Law Reform," 2024.
- ⁹⁵TechCrunch, "Google Search and Its Play Store App Marketplace Are Suspected of Breaching the EU's Digital Markets Act (DMA)," March 19, 2025.
- ⁹⁶European Commission, "Commission Sends Preliminary Findings to Meta over Its 'Pay or Consent' Model for Breach of the Digital Markets Act," July 1, 2024.
- ⁹⁷European Commission, "Commission Fines Apple €500 Million and Meta €200 Million for Breaches of the Digital Markets Act," April 23, 2025; see also Reuters, April 23, 2025.
- ⁹⁸Reuters. "Apple Fined \$570 Million and Meta \$228 Million for Breaching EU Law." April 23, 2025.
- ⁹⁹European Commission, "Commission Welcomes Apple's Commitments to Enable Alternative App Stores and Sideloads on iOS in Compliance with the DMA," January 25, 2024.
- ¹⁰⁰European Commission, "Commission Welcomes WhatsApp's Steps to Implement Interoperability Obligations Under the Digital Markets Act," March 6, 2024.
- ¹⁰¹European Commission, "Commission Welcomes Google's Proposed Compliance Measures Under the Digital Markets Act, Including Choice Screens and Data Separation Commitments," March 25, 2024.
- ¹⁰²GWJ & McAfee, Global Digital Trust Survey 2025: Navigating the New App Ecosystem, June 2025.
- ¹⁰³"For Developers, New App Stores Mean New Headaches," The Verge, March 15, 2025.
- ¹⁰⁴European DIGITAL SME Alliance, quoted in Financial Times, "Small Firms Say EU's Big Tech Law Has Yet to Deliver Benefits," May 6, 2024.
- ¹⁰⁵"Thanks to the European Union's DMA, Apple Has to Allow the Hot Tubs Porn App on iPhones," Apple World Today, February 20, 2025.
- ¹⁰⁶Vietnam, Law No. 19/2023/QH15 on Protection of Consumers' Rights.
- ¹⁰⁷Indonesia, Minister of Trade Regulation No. 31 of 2023.
- ¹⁰⁸P. Srinivasan, "ASEAN's Cautious Path on Digital Competition," Tech for Good Institute, 2024.
- ¹⁰⁹A. Wicaksono, "Aligning Indonesia's Digital Governance with Global Standards," Tech for Good Institute, 2024.
- ¹¹⁰M. Pangestu, "Getting ASEAN's Digital Trade Rules Right," East Asia Forum, 2023.
- ¹¹¹Government of Japan, Act on Promotion of Competition for Specified Smartphone Software, 2024.
- ¹¹²The Treasury, Australian Government, Regulating Digital Platforms: Consultation on a New Competition and Consumer Framework, 2024.
- ¹¹³Republic of Korea, Telecommunications Business Act (Amendment 2021).
- ¹¹⁴Competition and Consumer Commission of Singapore (CCCS), Guidelines on Price Transparency, 2022.
- ¹¹⁵Australian Government, Consumer Data Right (cdr.gov.au).
- ¹¹⁶Australian Competition & Consumer Commission (ACCC), ACCC Rejects ANZ's Proposed Acquisition of Suncorp Bank, 2023; Japan Fair Trade Commission (JFTC), Guidelines Concerning Administrative Procedures for Business Combination Reviews (2019).
- ¹¹⁷Australian Competition & Consumer Commission (ACCC). (2020-2025). Digital Platform Services Inquiry. This inquiry provides an in-depth analysis of the complexities of regulating algorithmic ranking and the potential for unintended consequences for both consumers and small businesses.
- ¹¹⁸Global Cross-Border Privacy Rules Forum. "Global CBPR Forum Declaration." April 21, 2022. <https://www.globalcbpr.org/documents>.

- ¹¹⁹Asian Development Bank (ADB). (2023). Asia Small and Medium-Sized Enterprise Monitor 2023.
- ¹²⁰Google, Temasek, and Bain & Company. (2023). e-Conomy SEA 2023 Report.
- ¹²¹Information Technology and Innovation Foundation (ITIF). (2022). The Dangers of Mandated Interoperability in the Digital Platform Economy. This analysis argues that such requirements can impose significant security risks and compliance costs that may disproportionately affect smaller firms.
- ¹²²Organisation for Economic Co-operation and Development (OECD). (2021). Regulatory Policy in Southeast Asia: Towards a New Agenda. This report discusses the ongoing need to build institutional capacity, resources, and expertise within regulatory agencies in the region to effectively oversee complex sectors.
- ¹²³Economic Research Institute for ASEAN and East Asia (ERIA). (2023). Study on the ASEAN Digital Economy Framework Agreement (DEFA). Policy Brief. Reports on DEFA frequently highlight the economic costs of regulatory fragmentation and the benefits of creating a harmonized digital market in the region.
- ¹²⁴Organisation for Economic Co-operation and Development (OECD). (2023). The Impact of Regulation on Innovation. This report discusses how prescriptive regulatory requirements can divert R&D resources toward compliance activities, potentially slowing the pace of innovation and product development cycles.
- ¹²⁵World Bank. (2023). Digital Progress and Trends Report. Reports from the World Bank on digitalization often discuss the barriers faced by MSMEs in emerging economies, including regulatory hurdles that can complicate their ability to participate in online platforms.
- ¹²⁶Information Technology and Innovation Foundation (ITIF). (2023). The Consumer Welfare Costs of Digital Platform Regulation. This analysis argues that certain regulatory interventions, such as forced unbundling, can lead to degraded product quality, reduced convenience, and potentially higher prices for consumers.
- ¹²⁷APEC Business Advisory Council (ABAC). (2024). Report to APEC Economic Leaders. This annual report consistently highlights that MSMEs constitute over 98% of businesses and a majority of employment in the APEC region, urging policymakers to adopt proportionate, context-sensitive regulations that support their growth.
- ¹²⁸eMarketer/Insider Intelligence. (2023). Retail and E-Commerce in Southeast Asia.
- ¹²⁹Google, Temasek, and Bain & Company. (2022–2024). e-Conomy SEA Reports.
- ¹³⁰JP Morgan. (2022). Global Payments Report 2022.
- ¹³¹Dentsu. (2023, 2024). Global Ad Spend Forecasts.
- ¹³²GroupM. (2023). This Year, Next Year: Global End-of-Year Forecast.
- ¹³³Statista. (2024). Digital Advertising Market Data, Country Profiles (APAC).
- ¹³⁴APEC Secretariat, “APEC Economies Step Up Cooperation on Digital Policy Challenges,” APEC News Release, July 30, 2025. Available at: <https://www.apec.org/press/news-releases/2025/apec-economies-step-up-cooperation-on-digital-policy-challenges>

