Luther.

Blogpost

Digital Business Models in Thailand, Vietnam and Singapore: Regulation as Part of a Market Entry Strategy

Digital Business Models, Platform Regulation and Market Access in Thailand, Vietnam and Singapore



Digital Platforms: Compliance Becomes an Architectural Issue

Digital platforms are increasingly the focus of competition, consumer protection, data protection and sector-specific regulation in the APAC region. Unlike the European Union, with its **Digital Markets Act ("DMA")**, the jurisdictions considered here have so far generally not adopted a unified gatekeeper regime. Instead, authorities apply existing instruments to data-driven business models, algorithmic decision-making and platform relationships. Platform architecture itself is therefore becoming a compliance factor.

This brings not only traditional questions of market power to the fore. Ranking and recommendation systems, data access, interoperability, pricing and commercial terms, as well as the design of user interfaces, are also relevant. Self-preferencing, anti-steering, tying and bundling, as well as opaque or manipulative design choices, may simultaneously trigger competition, data protection and consumer protection risks. This is particularly true with regard to defaults, visibility and the technical integration of a platform's own or affiliated services.

For internationally active companies, this means that market entry and digital compliance should not be planned separately. The business model, corporate and ownership structure, data flows, product design, contracts and dispute resolution should be aligned from the structuring phase onwards.

Germany: Platform Regulation as a Familiar Reference Framework

Companies with experience in the German and European markets will already be familiar with the principle that digital platforms are not assessed solely on the basis of their contractual arrangements. Product design, data flows, algorithmic controls and the specific user journey may themselves give rise to compliance requirements. This experience provides a useful starting point for market entry in the APAC region. It must, however, be adapted to the relevant local legal frameworks, administrative practice and market conditions.

Transparency in Platform-to-Business Relationships

The **Platform-to-Business (P2B) Regulation (EU) 2019/1150** requires, among other things, transparency regarding the main parameters determining rankings, communication of changes to terms and conditions, and comprehensible procedures for restrictions or suspensions of business accounts. Where platform operators differentiate between their own or affiliated offerings and those of business users, that differentiation must also be disclosed transparently.

The **Digital Services Act ("DSA")** is linked to the specific design and organisation of digital services. Depending on the nature and size of the service, platforms may in particular be required to provide reasons for content moderation decisions in a comprehensible manner and to maintain internal complaint-handling mechanisms. Decisions to remove or restrict content and user accounts should therefore be based on clear rules and documented in a manner that enables them to be explained to the affected parties.

Further DSA requirements concern the transparency of advertising and recommender systems. Users should be able to identify when advertising is displayed to them, on whose behalf it is displayed, and the main parameters used to recommend content or offerings. Consequently, not only legal texts but also data flows, algorithmic controls and the specific user interface become relevant components of compliance. The DSA also addresses designs that deceive or manipulate users or materially impair their ability to make a free and informed decision, for example through misleading choice architectures.

Germany's Digital Services Act (*Digitale-Dienste-Gesetz*, "**DDG**") supplements the DSA at national level. In particular, it governs domestic implementation and the responsibilities of the authorities involved. The substantive obligations for digital services arise largely directly from the DSA; the DDG provides the institutional and procedural framework for its application and enforcement in Germany. The Federal Network Agency (*Bundesnetzagentur*) acts as Germany's Digital Services Coordinator and performs central coordination and supervisory functions.

Data Protection and Consent Design

Consent design is a legally relevant product decision in Germany. The General Data Protection Regulation ("**GDPR**") and the Federal Data Protection Act (*Bundesdatenschutzgesetz*, "**BDSG**") provide the general data protection framework. For tracking technologies and for storing information on, or gaining access to information already stored in, users' terminal equipment, Section 25 of the Telecommunications Digital Services Data Protection Act (*Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz*, "**TDDDG**") may additionally apply. The validity of consent therefore depends not only on the wording used, but also on the specific design of the choice process.

Manipulative user interfaces may undermine the voluntary and informed nature of consent. This applies in particular to pre-selected options, asymmetrically designed buttons and unnecessarily burdensome refusal or withdrawal processes. Such designs may simultaneously engage several regulatory regimes:

- the DSA prohibition on manipulative design for online platforms;
- Sections 3, 5, 5a and 5b of the German Act Against Unfair Competition ("**UWG**"), together with the annex to Section 3(3) UWG;
- transparency and information obligations under Sections 312 et seq. of the German Civil Code ("**BGB**") and the Introductory Act to the Civil Code ("**EGBGB**");
- standard terms control under Sections 305 et seq. BGB; and
- where applicable, requirements concerning the cancellation button, order button and fixed-term contracts.

This illustrates that a single product design may create data protection, unfair competition, consumer contract and

platform-regulation risks at the same time. For internationally active companies, established processes involving data protection, product development, legal and compliance teams can therefore provide a sound basis. For entry into Thailand, Vietnam or Singapore, however, these processes should be integrated at an early stage and tailored to the local platform architecture, user journey and regulatory framework.

Thailand: Platform Regulation and Structured Market Entry

Thailand is a significant investment and business hub in Southeast Asia. Alongside an established industrial base and strong infrastructure, data centres, digital infrastructure, cloud services, semiconductors and advanced electronics are becoming increasingly important. This creates opportunities for regional headquarters, manufacturing, distribution, services and technology-driven business models.

At the same time, market entry is legally and administratively demanding. Foreign ownership restrictions, required permits, data protection, competition law, tax and employment issues, as well as a robust dispute resolution strategy, should therefore be assessed at an early stage. In practice, administrative procedures, local interpretative practice and documentation that may only be available in Thai can materially affect timing and implementation.

Platforms and Competition Law

In March 2026, the Trade Competition Commission of Thailand issued Guidelines for Multi-Sided Platform Businesses in the field of e-commerce. They clarify the application of the **Trade Competition Act B.E. 2560 (2017) ("TCA")** to digital platform models that connect different user groups through electronic systems. This may, for example, include online marketplaces, food delivery, ride-hailing, payment, logistics and advertising platforms.

The focus is on practices such as self-preferencing, meaning algorithmic control of visibility and rankings, rate-parity clauses, discriminatory fees or terms, tying and bundling, requirements to use particular logistics or payment services, and the use of third-party data to benefit a platform's own offerings.

However, the Guidelines do not establish a DMA-style ex ante regime. Rather, they support the case-by-case application of existing rules on abuse of a dominant market position, anti-competitive agreements and unfair trade practices (Sections 50, 54, 55, 57 and 58 TCA). Market conditions and competitive effects, the impact on consumers and market participants, and potential objective, technical or economic justifications remain decisive.

Section 57 TCA and merger control also warrant particular attention. Section 57 TCA may capture unfair trade practices even below the threshold of a dominant market position, for example the abuse of superior bargaining power, unjustified contractual changes, or unreasonable payment, rebate and tying terms. A hybrid control system applies to mergers (Section 51 TCA): certain transactions require prior approval, while others must be notified after completion within seven days.

Foreign Majority Shareholding, BOI Incentives and Nominee Risks

Foreign investors often use a private limited company to enter the Thai market, or for preparatory and support activities only, a representative office or regional office. The appropriate structure depends on the specific nature of the planned business activity, the proposed scale of operations and the relevant regulatory requirements.

The **Foreign Business Act B.E. 2542 (1999) ("FBA")** generally deems companies to be "foreign" where foreign natural or legal persons hold at least 50% of their shares. For such "foreign" companies, certain business activities are subject to restrictions and/or licensing requirements. Particularly in relation to platform models, careful classification is required, as they often combine different regulated activities, such as intermediation, payment services, logistics, advertising, data processing and technical support services, which typically require a **Foreign Business License ("FBL")**.

For eligible projects, promotion by the **Thai Board of Investment ("BOI")** may provide a preferred pathway to majority foreign ownership. In such cases, a Foreign Business Certificate may be obtained in lieu of a Foreign Business License through a simplified procedure. Depending on the project and the applicable promotion category, BOI promotion may, in addition to allowing up to 100% foreign ownership, provide various incentives, including tax holidays, customs exemptions, and facilitation with regard to visas and work permits. Eligibility for BOI promotion depends, among other

things, on the nature of the business activity, the investment amount, the level of technology, the location of the project, and compliance with the applicable BOI conditions.

So-called "Nominee" structures, on the other hand, should be strictly avoided. If Thai shareholders hold the majority of the shares merely as nominees or in a fiduciary capacity for a foreign investor, in order to enable the foreign investor to effectively operate a business that is otherwise restricted under the FBA, this may constitute a violation of Section 36 of the FBA. This is particularly the case if the Thai shareholders are merely nominally involved and the foreign investor provides the financing and assumes the economic interests and actual control over the company.

In addition to fines and imprisonment, this may result in the court-ordered termination of the shareholding arrangement or the business activities. The relevant assessment does not depend solely on the formal shareholding structure, but also takes into account the beneficial ownership, the financing and the actual governance of the company. Since early 2026, the Thai authorities have significantly intensified their enforcement efforts against such structures. For example, in connection with the incorporation of companies and capital increases involving foreign participation, the competent **Department of Business Development ("DBD")** now requires evidence of the source of funds contributed by the Thai shareholders, such as bank statements covering the preceding months.

Data Protection and Dispute Resolution

The **Personal Data Protection Act B.E. 2562 (2019) ("PDPA")** has been fully enforceable since June 2022. It may also apply to foreign businesses where they offer goods or services to individuals in Thailand or monitor their behaviour (Section 5 PDPA), for example through online services or targeted marketing. For cross-border data transfers to regional headquarters, group companies, shared service centres or cloud systems, the transfer mechanisms permitted under the PDPA must be reviewed and documented. Data protection due diligence and compliance should therefore cover customer and employee data, consent mechanisms, website and online tracking, CCTV, service-provider agreements, deletion concepts and international data transfers.

For high-value or cross-border contracts, dispute resolution should already be considered at the contracting stage. Thailand is a contracting state to the New York Convention, meaning that foreign arbitral awards are generally enforceable in Thailand (and vice versa). By contrast, foreign civil judgments are not directly enforceable in Thailand; the underlying claim must be re-litigated before the Thai courts, which may take the foreign judgment into consideration as evidence. Arbitration is therefore often attractive in international contracts, particularly because the parties can flexibly determine the rules, seat, language and composition of the arbitral tribunal.

Vietnam: Data Protection, Platform Design and Market Access

Vietnam does not yet have a uniform DMA-style regulatory framework. Instead, requirements for digital business models arise from the interaction of data protection, competition and consumer protection law, e-commerce regulation and sector-specific rules.

Data Protection, Consent and Cross-Border Data Transfers

Since 1 January 2026, the **Law on Personal Data Protection, Law No. 91/2025/QH15 ("PDPL")**, and its implementing regulation, **Decree No. 356/2025/ND-CP**, have formed the core of Vietnam's data protection framework. For platforms, consent under Article 9 PDPL is particularly relevant: it must be voluntary, informed, unambiguous and given for the specific processing purpose; silence is not sufficient. Pre-ticked consent is expressly prohibited. Consent design is therefore a key compliance issue. Bundled consent, the unequal prominence of options or unnecessarily difficult choice mechanisms may undermine the validity of consent, particularly in connection with personalisation, targeted advertising and AI-based recommendations.

Data protection law also imposes extensive organisational and documentation obligations. As a rule, controllers must prepare a data protection impact assessment dossier and submit it to the competent specialised authority of the Ministry of Public Security within 60 days of the start of processing. They must also implement technical and organisational security measures and appoint qualified data protection personnel or engage an external data protection service provider. Comparable requirements apply to cross-border data transfers, which include foreign hosting, cloud services and intra-group data flows outside Vietnam. Data flows, hosting architecture and intra-group access arrangements

should therefore be identified and documented at an early stage. Certain small enterprises and start-ups benefit from limited relief until the end of 2030.

Since 19 August 2026, **Decree No. 330/2026/ND-CP** has governed administrative fines for violations of data protection and cybersecurity law. For most data protection violations, the maximum fine for companies is VND 3 billion. Article 56 provides for turnover-based fines only in relation to certain serious infringements involving cross-border data transfers: transfers made without the required data protection impact assessment dossier, concealed or falsely declared data flows, and the continuation of a prohibited transfer. Where such an infringement results in the leakage or loss of data relating to at least 10,000 Vietnamese data subjects, the fine ranges from 1% to 5% of the company's total turnover in the Vietnamese market in the preceding financial year, depending on the number of affected individuals. If there is no such turnover, or if the calculated amount would be less than VND 3 billion, fixed fine ranges apply instead. In addition, the cross-border transfer may be suspended for six to twelve months, and the authority may order remedial measures.

Consumer Protection and E-Commerce

Consumer protection law imposes further requirements. The **Law on Protection of Consumer Rights, Law No. 19/2023/QH15**, requires operators of digital intermediary platforms, among other things, to identify sellers, provide transparent information, handle consumer reviews appropriately and operate complaint-handling procedures. Large digital platforms must also regularly assess their systems for algorithmically targeted advertising, the handling of fake accounts and the use of AI and automated processes.

Since 1 July 2026, the **E-Commerce Law, Law No. 122/2025/QH15,** and **Decree No. 248/2026/ND-CP** have also been in force. These rules extend to foreign providers and, depending on the platform's functions and business model, impose in particular registration, platform-policy and seller-verification obligations. The relevant classification depends, for example, on whether the service qualifies as an intermediary platform, a social-commerce platform or a livestream sales platform. Electronic identity verification of sellers will apply from 1 January 2027.

Competition Law and Market Access

Vietnam's Competition Law, **Law No. 23/2018/QH14**, covers, among other things, anti-competitive agreements, the abuse of dominant market positions and forms of unfair competition. There is currently no standalone gatekeeper regime. Rankings, exclusivity arrangements, access to data and preferential treatment of a platform operator's own or affiliated offerings are not unlawful per se. However, they must be assessed in light of the platform operator's market position and the specific market conditions.

For operational activities, the principal options are generally a Limited Liability Company or a Joint Stock Company; depending on the business model, a Business Cooperation Contract structure may also be appropriate. A representative office is not an equivalent alternative: it may carry out liaison and market-research activities but may not undertake directly profit-generating activities. **Decree No. 248/2026/ND-CP** also provides for a national-security review of controlling interests in large digital platforms.

Before entering the market, companies should therefore assess, in particular, their data flows and consent processes, the platform's specific role and functions, and applicable e-commerce, payment, telecommunications and other sector-specific licensing requirements.

Singapore: Product Governance, Data and Sector-Specific Regulation

Singapore is an important location for regional headquarters, digital services, payment models and technology-driven business models. Its regulatory environment is innovation- and application-oriented, combining binding requirements with guidance, industry collaboration and testing formats. This openness is nevertheless accompanied by clear expectations concerning data processing, AI governance, online safety, cybersecurity, and financial and payment services.

Online Safety and Plattform-Governance

For designated app distribution services, product design is increasingly becoming a compliance issue. The **Infocomm Media Development Authority's Code of Practice for Online Safety** has been in effect for designated app distribution services since 31 March 2025. Systemic measures are required to reduce the risk of harmful content, with a

particular focus on protecting children. Therefore, online safety, user communications and risk management are all part of product governance.

Data Protection and AI Governance

The **Personal Data Protection Act 2012** provides the general data protection framework. Under Personal Data Protection Commission guidance on the use of personal data in generative AI, the system deployer bears central responsibility. Companies should therefore transparently define roles, purposes, categories of data, safeguards and withdrawal options, particularly in connection with training and fine-tuning and the integration of external models, APIs, cloud providers and system integrators. Productive AI and agentic systems should also be subject to risk-appropriate approvals, human control points and logging.

The use of agentic AI systems warrants particular attention. Unlike purely assistive AI tools, such systems may independently plan tasks, use external tools, retrieve data and trigger actions in digital processes. The compliance focus therefore shifts from the quality of individual outputs to the governance of permissions, access to tools and data, escalation mechanisms and the actual consequences of system actions.

Before deployment, companies should therefore define which decisions an AI system may prepare or execute autonomously, when human approval is required, and how inputs, system actions and outcomes will be logged. Risk assessments, limitations on autonomy and access rights, clearly defined control points, and ongoing testing and access restrictions should form part of the governance framework for productive agentic systems. This may be particularly relevant for applications in customer service, procurement, sales, HR, software development, payment operations or compliance monitoring.

Payments and Cybersecurity

For payment, wallet, marketplace or token-related business models, it should be clarified at an early stage whether the company's specific role involves regulated payment services.

Depending on the model's substance and actual role, these may include facilitating or executing payment transactions, issuing or transferring e-money, cross-border money transfers, or account and payment-initiation functions. By contrast, Digital Payment Token Services may cover business models involving dealing in, transferring or holding digital payment tokens. The relevant assessment is not based on the product label, but on the company's actual role in the flow of funds or tokens. The licensing and supervisory regime of the **Monetary Authority of Singapore** should therefore be reviewed before operational implementation. Due to the scope of their activities, major payment institutions are subject to additional requirements, particularly with regard to safeguarding customer funds.

Cybersecurity should be addressed as an integrated legal and contractual review point, particularly in relation to cloud outsourcing, group-wide access rights, incident response, and critical or infrastructure-relevant services.

Practical Checklist: What Companies Should Review

- **Platform design:** Rankings, recommendations, defaults, delisting and account suspensions must be transparent, consistent and objectively justifiable. German processes and best practices can serve as a starting point, but must be adapted to the respective target market.
- **Terms and conditions:** Rate-parity clauses, pricing requirements, tying arrangements, fees, and rebate and campaign requirements should be reviewed under competition law.
- **Data strategy:** Data flows, consent processes, third-party access, AI training and international transfers must be documented and legally safeguarded.
- **Market entry structure:** The legal form, foreign ownership, permits, eligibility for BOI promotion and sector-specific regulation must be reconciled before operations commence.
- **Governance:** Responsibilities for product decisions, algorithms, data protection, cybersecurity and regulatory communications should be clearly allocated.
- **Contracts and enforcement:** Governing law, jurisdiction, arbitration clauses, enforceability and interim relief should form part of early contract planning.

Conclusion

Thailand, Vietnam and Singapore do not follow a uniform DMA replica.

Nevertheless, digital business models in all three markets are increasingly shaped by the interaction of competition, data protection, security, consumer protection and sector-specific regulation. Uniform group standards or best practices developed for the German market are a sensible starting point, but they are not sufficient. They must be adapted to the relevant platform architecture, data use, security organisation, market structure and payment flows.

For international companies, the key lies in integrated implementation: those that bring together market entry, product design, data strategy, governance and contractual structure from the outset will reduce regulatory risks and establish a more robust basis for digital growth in the APAC region.

Your contact persons:



Dr Stefanie Hellmich, LL.M.
Lawyer, Partner
Frankfurt a.M.
+49 69 27229 24118
stefanie.hellmich@luther-lawfirm.com



Julia Hartung, Maîtrise en Droit
Lawyer, Senior Associate
Singapore
+65 6408 8000
julia.hartung@luther-lawfirm.com



Fabian Lorenz, M.A.
Lawyer, Partner, Location Head
Bangkok
+66 61 420 4049
fabian.lorenz@luther-lawfirm.com



Dr Tino Haupt
Lawyer, Senior Associate
Ho Chi Minh City
+84 28 7300 1073
tino.haupt@luther-lawfirm.com



Dr Maximilian Kressner, M.Jur. (Oxford)
Attorney-at-Law, Partner
Singapore
+65 6408 8000
maximilian.kressner@luther-lawfirm.com



Sabrina Aurnhammer
Lawyer | Associate
Munich
+49 89 23714 21668
sabrina.aurnhammer@luther-lawfirm.com



Leif Dustin Schneider
Lawyer, Counsel, Registered foreign lawyer (Vietnam)
Ho Chi Minh City
+84 (0)28 7300 1073
leif.schneider@luther-lawfirm.com



Deike Tamm
Lawyer, Associate
Frankfurt a.M.
+49 69 27229 14067
deike.tamm@luther-lawfirm.com



Birgitta von Dresky
Lawyer, Partner, Location Head
Singapore
+65 6408 8008
birgitta.von.dresky@luther-lawfirm.com



Tim Tewes
Lawyer, Attorney-at-Law (Germany), Associate
Bangkok
+66 93 586 6669
tim.tewes@luther-lawfirm.com

Release: October 2026