Luther.

Blogbeitrag

Digitale Geschäftsmodelle in Thailand, Vietnam und Singapur: Regulierung als Teil der Markteintrittsstrategie

Digitale Geschäftsmodelle, Plattformregulierung und Marktzugang in Thailand, Vietnam und Singapur



Digitale Plattformen: Compliance wird zur Architekturfrage

Digitale Plattformen stehen in der APAC-Region zunehmend im Fokus von Wettbewerbs-, Verbraucherschutz-, Datenschutz- und Sektorregulierung. Anders als die Europäische Union mit dem **Digital Markets Act („DMA“)** setzen die hier betrachteten Jurisdiktionen bislang überwiegend nicht auf ein einheitliches Gatekeeper-Regime. Stattdessen wenden die Behörden bestehende Instrumente auf datengetriebene Geschäftsmodelle, algorithmische Steuerung und Plattformbeziehungen an. Plattformarchitektur wird damit selbst zum Compliance-Faktor.

Dadurch rücken nicht nur klassische Fragen der Marktmacht in den Vordergrund. Relevant sind auch Ranking- und Empfehlungssysteme, Datenzugang, Interoperabilität, Preis- und Konditionenmodelle sowie die Gestaltung von Nutzeroberflächen. Self-Preferencing, Anti-Steering, Tying und Bundling ebenso wie intransparente oder manipulative Designentscheidungen können zugleich wettbewerbs-, datenschutz- und verbraucherschutzrechtliche Risiken auslösen. Dies gilt insbesondere für Defaults, Sichtbarkeit und die technische Einbindung eigener oder verbundener Dienste.

Für international tätige Unternehmen folgt daraus: Markteintritt und Digital Compliance sollten nicht getrennt voneinander geplant werden. Geschäftsmodell, Gesellschafts- und

Eigentümerstruktur, Datenflüsse, Produktdesign, Verträge und Streitbeilegung sollten bereits in der Strukturierungsphase aufeinander abgestimmt werden.

Deutschland: Plattformregulierung als vertrauter Referenzrahmen

Unternehmen mit Erfahrungen im deutschen und europäischen Markt kennen bereits den Grundgedanken, dass digitale Plattformen nicht allein anhand ihrer Verträge bewertet werden. Vielmehr können Produktgestaltung, Datenflüsse, algorithmische Steuerung und die konkrete Nutzerführung eigenständige Compliance-Anforderungen auslösen. Diese Erfahrungen bieten für den Markteintritt in der APAC-Region einen hilfreichen Ausgangspunkt. Sie müssen jedoch an die jeweiligen lokalen Rechtsrahmen, Behördenpraxis und Marktgegebenheiten angepasst werden.

Transparenz in Plattform-B2B-Beziehungen

Die **Platform-to-Business-Verordnung (P2B-Verordnung) 2019/1150** verlangt unter anderem Transparenz über wesentliche Parameter von Rankings, die Kommunikation von Änderungen der Geschäftsbedingungen sowie nachvollziehbare Verfahren bei Einschränkungen oder Sperrungen von Geschäftskonten. Soweit Plattformbetreiber eigene oder verbundene Angebote gegenüber denen gewerblicher Nutzer unterschiedlich behandeln, ist auch diese Differenzierung transparent darzustellen.

Der **Digital Services Act („DSA")** knüpft an die konkrete Ausgestaltung und Organisation digitaler Dienste an. Abhängig von Art und Größe des Dienstes können Plattformen insbesondere verpflichtet sein, Moderationsentscheidungen nachvollziehbar zu begründen und interne Beschwerdemöglichkeiten vorzuhalten. Entscheidungen über die Entfernung oder Einschränkung von Inhalten und Nutzerkonten sollten daher auf klaren Regeln beruhen und so dokumentiert werden, dass sie gegenüber Betroffenen erläutert werden können.

Weitere DSA-Anforderungen betreffen die Transparenz von Werbung und Empfehlungssystemen. Nutzer sollen erkennen können, wann ihnen Werbung angezeigt wird, in wessen Auftrag dies erfolgt und nach welchen wesentlichen Kriterien Inhalte oder Angebote empfohlen werden. Damit werden nicht nur Rechtstexte, sondern auch Datenflüsse, algorithmische Steuerung und die konkrete Nutzeroberfläche zu relevanten Compliance-Bestandteilen. Der DSA adressiert zudem Gestaltungen, die Nutzer täuschen, manipulieren oder ihre freie und informierte Entscheidung wesentlich beeinträchtigen können, etwa durch irreführende Auswahlmöglichkeiten.

Das deutsche **Digitale-Dienste-Gesetz („DDG")** ergänzt den DSA auf nationaler Ebene. Es regelt insbesondere dessen innerstaatliche Durchführung und die Zuständigkeiten der beteiligten Behörden. Die materiellen Pflichten für digitale Dienste ergeben sich dabei im Wesentlichen unmittelbar aus dem DSA; das DDG schafft den institutionellen und verfahrensrechtlichen Rahmen für dessen Anwendung und Durchsetzung in Deutschland. Die Bundesnetzagentur fungiert dabei als deutsche Koordinierungsstelle für digitale Dienste und nimmt zentrale Koordinierungs- und Aufsichtsaufgaben wahr.

Datenschutz und Consent Design

Consent Design ist in Deutschland eine rechtlich relevante Produktentscheidung. Die **Datenschutz-Grundverordnung („DSGVO")** und das **Bundesdatenschutzgesetz (BDSG)** bilden den allgemeinen datenschutzrechtlichen Rahmen. Für Tracking-Technologien sowie das Speichern von Informationen in Endgeräten oder den Zugriff auf solche Informationen kann zusätzlich § 25 des **Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz („TDDDG")** einschlägig sein. Ob eine Einwilligung wirksam ist, hängt daher nicht nur vom Wortlaut, sondern auch von der konkreten Gestaltung des Auswahlprozesses ab.

Manipulative Nutzeroberflächen können die Freiwilligkeit und Informiertheit einer Einwilligung beeinträchtigen. Dies betrifft insbesondere voreingestellte Auswahlmöglichkeiten, asymmetrisch gestaltete Schaltflächen sowie unnötig erschwerte Ablehnungs- oder Widerrufswege. Solche Gestaltungen können zugleich mehrere Regelungsbereiche berühren:

- das Verbot manipulativer Gestaltung nach dem DSA für Online-Plattformen;
- die §§ 3, 5, 5a und 5b des **Gesetzes gegen den unlauteren Wettbewerb („UWG")** sowie den Anhang zu § 3 Abs. 3 UWG;
- Transparenz- und Informationspflichten nach den §§ 312 ff. BGB und dem EGBGB;
- die AGB-Kontrolle nach §§ 305 ff. BGB; sowie
- gegebenenfalls Vorgaben zum Kündigungsbutton, Bestellbutton und zu Laufzeitverträgen.

Dies verdeutlicht, dass ein und dieselbe Produktgestaltung zugleich datenschutzrechtliche, lauterkeitsrechtliche, verbrauchervertragsrechtliche und plattformregulatorische Risiken begründen kann. Für international tätige Unternehmen können etablierte Prozesse aus Datenschutz, Produktentwicklung, Legal und Compliance deshalb eine tragfähige Grundlage sein. Für den Eintritt in Thailand, Vietnam oder Singapur sollten diese Prozesse jedoch frühzeitig zusammengeführt und auf die dortige Plattformarchitektur, Nutzerführung und lokale Regulierung zugeschnitten werden.

Thailand: Plattformregulierung und strukturierter Markteintritt

Thailand ist ein bedeutender Investitions- und Wirtschaftshub in Südostasien. Neben einer etablierten industriellen Basis und einer leistungsfähigen Infrastruktur gewinnen insbesondere Rechenzentren, digitale Infrastruktur, Cloud Services, Halbleiter und Advanced Electronics zunehmend an Bedeutung. Dadurch ergeben sich Chancen für regionale Headquarters, Produktion, Distribution, Dienstleistungen und technologiegetriebene Geschäftsmodelle.

Gleichzeitig ist der Markteintritt rechtlich und administrativ anspruchsvoll. Ausländische Beteiligungsbeschränkungen, erforderliche Genehmigungen, Datenschutz, Kartellrecht, Steuer- und Beschäftigungsfragen sowie eine tragfähige Streitbeilegungsstrategie sollten daher frühzeitig geprüft werden. In der Praxis können administrative Verfahren, lokale Auslegungspraxis und Unterlagen, die teils nur in thailändischer Sprache vorliegen, Timing und Umsetzung erheblich beeinflussen.

Plattformen und Kartellrecht

Die Trade Competition Commission of Thailand hat im März 2026 Guidelines für Multi-Sided Platform Businesses im Bereich E-Commerce veröffentlicht. Diese konkretisieren die Anwendung des **Trade Competition Act B.E. 2560 (2017) („TCA“)** auf digitale Plattformmodelle, die verschiedene Nutzergruppen über elektronische Systeme zusammenbringen. Beispiel hierfür sind Online-Marktplätze, Food-Delivery- und Ride-Hailing-Plattformen, die Kunden mit Händlern, Dienstleistern sowie Zahlungs- und Logistikanbietern verbinden.

Im Mittelpunkt stehen Praktiken wie Self-Preferencing, also die algorithmische Steuerung von Sichtbarkeit und Rankings, Rate-Parity-Klauseln, diskriminierende Gebühren oder Konditionen, Tying und Bundling, Vorgaben zur Nutzung bestimmter Logistik- oder Zahlungsdienste sowie die Nutzung von Daten Dritter zugunsten eigener Angebote.

Die Guidelines schaffen jedoch kein DMA-ähnliches Ex-ante-Regime. Sie dienen vielmehr der einzelfallbezogenen Anwendung bestehender Vorschriften über den Missbrauch einer marktbeherrschenden Stellung, wettbewerbsbeschränkende Vereinbarungen und unfaire Handelspraktiken (vgl. §§ 50, 54, 55, 57 und 58 TCA). Von entscheidender Bedeutung sind die Marktbedingungen und Wettbewerbswirkungen, die Auswirkungen auf Verbraucher und Marktteilnehmer sowie mögliche sachliche, technische oder wirtschaftliche Rechtfertigungen.

Besondere Aufmerksamkeit verdienen zudem § 57 TCA und die Fusionskontrolle. § 57 TCA kann unfaire Handelspraktiken auch unterhalb der Schwelle einer marktbeherrschenden Stellung erfassen, beispielsweise den Missbrauch überlegener Verhandlungsmacht, ungerechtfertigte Vertragsänderungen oder unangemessene Zahlungs-, Rabatt- und Koppelungsbedingungen. Bei Zusammenschlüssen gilt ein hybrides Kontrollsystem (§ 51 TCA): Bestimmte Transaktionen bedürfen einer vorherigen Genehmigung, während andere innerhalb von sieben Tagen nach Vollzug nachträglich angemeldet werden müssen.

Ausländische Unternehmensbeteiligung, BOI-Förderung und Nominee-Risiken

Ausländische Investoren nutzen für den Markteintritt in Thailand häufig eine Private Limited Company oder – für rein vorbereitende und unterstützende Tätigkeiten – ein Representative Office oder Regional Office. Welche Struktur geeignet ist, hängt von Inhalt und Umfang der konkreten unternehmerischen Tätigkeit und den dafür geltenden regulatorischen Anforderungen ab.

Der **Foreign Business Act B.E. 2542 (1999) („FBA“)** qualifiziert Unternehmen grundsätzlich als „ausländisch“, wenn ausländische natürliche oder juristische Personen mindestens 50 % der Unternehmensanteile halten. Für die Ausübung bestimmter Tätigkeiten durch solche „ausländischen“ Unternehmen gelten Beschränkungen und/oder Genehmigungspflichten. Insbesondere bei Plattformmodellen, die häufig verschiedene regulierte

Tätigkeiten und Leistungen wie Vermittlung, Zahlungsdienste, Logistik, Werbung, Datenverarbeitung und technische Unterstützungsleistungen verbinden, ist eine sorgfältige Einordnung erforderlich, da hierfür regelmäßig eine **Foreign Business License („FBL“)** erforderlich ist.

Für bestimmte Projekte kann auch eine Förderung durch das thailändische **Board of Investment („BOI“)** den Weg zu einer ausländischen Mehrheitsbeteiligung eröffnen. In diesem Fall tritt an die Stelle der FBL ein Foreign Business Certificate, das in einem vereinfachten Verfahren erteilt wird. Je nach Projekt und Förderungskategorie umfasst die BOI-Förderung neben der Möglichkeit einer bis zu 100-prozentigen ausländischen Beteiligung insbesondere steuerliche Anreize, Zollbefreiungen sowie Erleichterungen bei Visa und Arbeitsgenehmigungen. Maßgeblich für die Förderfähigkeit sind unter anderem die Tätigkeit, das Investitionsvolumen, das Technologieniveau, der Standort und die Einhaltung der jeweiligen BOI-Bedingungen.

Von sogenannten Strohmann-Strukturen ist hingegen dringend abzuraten. Wenn thailändische Anteilseigner die Mehrheit der Anteile lediglich treuhänderisch bzw. als „Nominees“ für einen ausländischen Investor halten, um diesem trotz der Beschränkungen des FBA die tatsächliche Ausübung eines grundsätzlich beschränkten Geschäfts zu ermöglichen, kann dies einen Verstoß gegen § 36 FBA darstellen. Dies gilt insbesondere, wenn die thailändischen Anteilseigner lediglich formal beteiligt sind und der ausländische Investor die Finanzierung, wirtschaftlichen Interessen und tatsächliche Kontrolle über das Unternehmen übernimmt. Neben Geld- und Freiheitsstrafen kann dies zur gerichtlich angeordneten Beendigung der Beteiligung bzw. der Geschäftstätigkeit führen. Maßgeblich sind dabei nicht allein die formalen Beteiligungsverhältnisse, sondern auch die wirtschaftliche Berechtigung, die Finanzierung und die tatsächliche Governance. Seit Anfang 2026 haben die thailändischen Behörden ihr Vorgehen gegen derartige Strukturen deutlich intensiviert. So verlangt das zuständige **Department of Business Development („DBD“)** bei der Gründung von Gesellschaften und bei Kapitalerhöhungen mit ausländischer Beteiligung inzwischen unter anderem Nachweise über die Herkunft der von den thailändischen Gesellschaftern eingebrachten Mittel, etwa in Form von Kontoauszügen der vorausgegangenen Monate.

Datenschutz und Streitbeilegung

Der **Personal Data Protection Act B.E. 2562 (2019) („PDPA“)** ist seit Juni 2022 vollständig durchsetzbar. Er kann auch ausländische Unternehmen erfassen, wenn sie Personen in Thailand Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten (§ 5 PDPA), etwa bei Online-Diensten, zielgerichtetem Marketing oder Verhaltensmonitoring. Bei grenzüberschreitenden Datenübermittlungen an regionale Headquarters, Konzerngesellschaften, Shared-Service-Center oder Cloud-Systeme müssen die nach dem PDPA zulässigen Transfermechanismen (§§ 28, 29 PDPA) geprüft und dokumentiert werden. Datenschutz-Due-Diligence und Compliance sollten daher Kundendaten, Beschäftigtendaten, Einwilligungsmechanismen, Website- und Online-Tracking, CCTV, Dienstleisterverträge, Löschkonzepte sowie internationale Datentransfers abdecken.

Bei hochwertigen oder grenzüberschreitenden Verträgen sollte die Streitbeilegung bereits bei Vertragsschluss berücksichtigt werden. Thailand ist Vertragsstaat des New Yorker Übereinkommens, sodass ausländische Schiedssprüche in Thailand grundsätzlich vollstreckbar sind (und umgekehrt). Ausländische Zivilurteile sind in Thailand hingegen nicht vollstreckbar; der Anspruch muss vor thailändischen Gerichten neu eingeklagt werden, wobei das ausländische Urteil als Beweismittel berücksichtigt werden kann. Schiedsgerichtsbarkeit ist deshalb bei internationalen Verträgen häufig attraktiv, zumal die Parteien Regeln, Sitz, Sprache und Zusammensetzung des Schiedsgerichts flexibel gestalten können.

Vietnam: Datenschutz, Plattformdesign und Marktzugang

Vietnam verfügt bislang über keinen einheitlichen DMA-ähnlichen Rechtsrahmen. Die Anforderungen an digitale Geschäftsmodelle ergeben sich vielmehr aus dem Zusammenspiel von Datenschutz-, Wettbewerbs- und Verbraucherschutzrecht, E-Commerce-Regulierung und sektorspezifischen Vorgaben.

Datenschutz, Einwilligung und grenzüberschreitende Datenübermittlungen

Seit dem 1. Januar 2026 bilden das Gesetz über den Schutz personenbezogener Daten, **Law No. 91/2025/QH15 („PDPL“)**,

und die dieses konkretisierende Durchführungsverordnung **Decree No. 356/2025/ND-CP** den Kern des vietnamesischen Datenschutzrahmens. Für Plattformen ist insbesondere die Einwilligung nach Art. 9 PDPL relevant: Sie muss freiwillig, informiert, eindeutig und für den jeweiligen Verarbeitungszweck erteilt werden; Schweigen genügt nicht. Voreingestellte Einwilligungen sind ausdrücklich untersagt. Consent Design ist damit eine zentrale Compliance-Frage. Gebündelte Einwilligungen, eine ungleiche Hervorhebung von Optionen oder unnötig erschwerte Auswahlmöglichkeiten können die Wirksamkeit einer Einwilligung gefährden, insbesondere bei Personalisierung, zielgerichteter Werbung und KI-gestützten Empfehlungen.

Das Datenschutzrecht enthält zudem weitreichende Organisations- und Dokumentationspflichten. Verantwortliche müssen für die Datenverarbeitung grundsätzlich ein Dossier zur Datenschutz-Folgenabschätzung erstellen und innerhalb von 60 Tagen nach Beginn der Verarbeitung bei der zuständigen Fachbehörde des Ministeriums für öffentliche Sicherheit einreichen. Hinzu kommen technische und organisatorische Sicherheitsmaßnahmen sowie qualifiziertes Datenschutzpersonal oder ein externer Datenschutzdienstleister. Vergleichbare Anforderungen gelten für grenzüberschreitende Datenübermittlungen, zu denen auch ausländisches Hosting, Cloud-Dienste und konzerninterne Datenflüsse außerhalb Vietnams zählen. Datenflüsse, Hosting-Architektur und konzerninterne Zugriffe sollten daher frühzeitig erfasst und dokumentiert werden. Für bestimmte kleine Unternehmen und Start-ups bestehen bis Ende 2030 begrenzte Erleichterungen.

Seit dem 19. August 2026 regelt **Decree No. 330/2026/ND-CP** die Geldbußen für Verstöße gegen das Datenschutz- und Cybersicherheitsrecht. Für die meisten Datenschutzverstöße liegt der Höchstbetrag für Unternehmen bei 3 Mrd. VND. Umsatzbezogene Geldbußen sieht Art. 56 nur für bestimmte schwerwiegende Verstöße bei grenzüberschreitenden Übermittlungen vor: Übermittlungen ohne das erforderliche Dossier zur Datenschutz-Folgenabschätzung, verschleierte oder falsch angegebene Datenflüsse sowie die Fortsetzung einer untersagten Übermittlung. Führt ein solcher Verstoß zum Abfluss oder Verlust von Daten von mindestens 10.000 vietnamesischen Betroffenen, beträgt die Geldbuße je nach deren Zahl 1 bis 5 % des Gesamtumsatzes auf dem vietnamesischen Markt im vorangegangenen Geschäftsjahr. Fehlt ein solcher Umsatz oder läge der errechnete Betrag unter 3 Mrd. VND, gelten feste Bußgeldrahmen. Zusätzlich kann die grenzüberschreitende Übermittlung für sechs bis zwölf Monate ausgesetzt werden, und die Behörde kann Abhilfemaßnahmen anordnen.

Verbraucherschutz und E-Commerce

Hinzu kommt das Verbraucherschutzrecht. Das Gesetz zum Schutz der Verbraucherrechte, **Law No. 19/2023/QH15**, verpflichtet Betreiber digitaler Vermittlungsplattformen insbesondere zur Identifizierung von Verkäufern, zur Bereitstellung transparenter Informationen, zum ordnungsgemäßen Umgang mit Verbraucherbewertungen und zur Bearbeitung von Beschwerden. Große digitale Plattformen müssen zusätzlich ihre Systeme für algorithmisch zielgerichtete Werbung, den Umgang mit Fake-Accounts sowie den Einsatz von KI und automatisierten Verfahren regelmäßig bewerten.

Seit dem 1. Juli 2026 gelten das E-Commerce-Gesetz, **Law No. 122/2025/QH15**, und **Decree No. 248/2026/ND-CP**. Die Vorschriften erfassen auch ausländische Anbieter und sehen – abhängig von Plattformfunktion und Geschäftsmodell – insbesondere Registrierungs-, Plattformrichtlinien- und Verkäuferprüfungspflichten vor. Entscheidend ist, ob das Angebot etwa als Vermittlungsplattform, Social-Commerce- oder Livestream-Verkaufsplattform einzuordnen ist. Die elektronische Identitätsprüfung von Verkäufern ist ab dem 1. Januar 2027 verpflichtend.

Wettbewerbsrecht und Marktzugang

Das vietnamesische Wettbewerbsgesetz, **Law No. 23/2018/QH14**, erfasst unter anderem wettbewerbsbeschränkende Vereinbarungen, den Missbrauch marktbeherrschender Stellungen und Formen unlauteren Wettbewerbs. Ein eigenständiges Gatekeeper-Regime besteht bislang nicht. Rankings, Exklusivitätsvereinbarungen, Datenzugang und die bevorzugte Behandlung eigener oder verbundener Angebote sind nicht per se unzulässig, müssen aber anhand der Marktstellung des Plattformbetreibers und der konkreten Marktverhältnisse geprüft werden.

Für operative Tätigkeiten kommen in erster Linie eine Limited Liability Company oder eine Joint Stock Company, je nach Geschäftsmodell auch eine Business-Cooperation-Contract-Struktur, in Betracht. Eine Repräsentanz ist keine gleichwertige Alternative: Sie kann Verbindungs- und

Marktforschungsaufgaben übernehmen, darf aber keine unmittelbar gewinnbringenden Tätigkeiten ausüben. Für beherrschende Beteiligungen an großen digitalen Plattformen sieht **Decree No. 248/2026/ND-CP** zudem eine Prüfung unter Gesichtspunkten der nationalen Sicherheit vor.

Vor dem Markteintritt sollten Unternehmen daher insbesondere Datenflüsse und Einwilligungsprozesse, die konkrete Rolle und Funktion der Plattform sowie einschlägige E-Commerce-, Zahlungs-, Telekommunikations- und sonstige sektorale Genehmigungspflichten prüfen.

Singapur: Produkt-Governance, Daten und sektorale Regulierung

Singapur ist ein wichtiger Standort für regionale Headquarters, digitale Dienstleistungen, Zahlungsmodelle und technologiegetriebene Geschäftsmodelle. Das regulatorische Umfeld ist innovations- und anwendungsorientiert und verbindet verbindliche Anforderungen mit Leitlinien, branchenbezogener Zusammenarbeit und Erprobungsformaten. Diese Offenheit geht jedoch mit klaren Anforderungen an Datenverarbeitung, KI-Governance, Online Safety, Cybersecurity sowie Finanz- und Zahlungsdienstleistungen einher.

Online Safety und Plattform-Governance

Für bestimmte App-Vertriebsdienste wird die Produktgestaltung zunehmend zu einer Compliance-Frage. Der **Verhaltenskodex für Online-Sicherheit der Infocomm Media Development Authority** gilt seit dem 31. März 2025 für bestimmte App-Vertriebsdienste. Er verlangt systemische Maßnahmen zur Verringerung der Risiken durch schädliche Inhalte, wobei der Schutz von Kindern besonders im Mittelpunkt steht. Damit sind Online-Sicherheit, Nutzerkommunikation und Risikomanagement integrale Bestandteile der Produkt-Governance.

Data Protection und AI Governance

Der **Personal Data Protection Act 2012** bildet den allgemeinen Datenschutzrahmen. Nach den Leitlinien der Personal Data Protection Commission zur Nutzung personenbezogener Daten in generativer KI kommt dem System Deployer eine zentrale Verantwortung zu. Unternehmen sollten daher insbesondere beim Training und Fine-Tuning sowie bei der Einbindung externer Modelle, APIs, Cloud-Provider und Systemintegratoren Rollen, Zwecke, Datenarten, Schutzmaßnahmen und Widerrufsmöglichkeiten transparent regeln. Für produktive KI- und Agentensysteme sollten zudem risikoadäquate Freigaben, menschliche Kontrollpunkte und Protokollierung vorgesehen werden.

Besondere Aufmerksamkeit verdient der Einsatz agentischer KI-Systeme. Anders als rein unterstützende KI-Tools können solche Systeme Aufgaben eigenständig planen, externe Tools nutzen, Daten abrufen und Handlungen in digitalen Prozessen auslösen. Damit verlagert sich der Compliance-Fokus von der Qualität einzelner Ausgaben auf die Steuerung von Berechtigungen, Tool- und Datenzugriffen, Eskalationsmechanismen sowie der tatsächlichen Handlungsfolgen.

Für Unternehmen bedeutet dies insbesondere, vor dem Einsatz festzulegen, welche Entscheidungen ein KI-System selbstständig vorbereiten oder ausführen darf, wann eine menschliche Freigabe erforderlich ist und wie Eingaben, Systemaktionen und Ergebnisse protokolliert werden. Risikobewertung, Einschränkung von Autonomie und Zugriffsrechten, klar definierte Kontrollpunkte sowie fortlaufende Tests und Zugriffsbeschränkungen sollten daher Teil der Governance für produktive Agentensysteme sein. Dies kann insbesondere für Anwendungen im Kundenservice, Einkauf, Vertrieb, HR, in der Softwareentwicklung, im Zahlungsverkehr oder im Compliance-Monitoring relevant sein.

Payments und Cybersecurity

Bei Zahlungs-, Wallet-, Marktplatz- oder tokenbezogenen Geschäftsmodellen ist frühzeitig zu klären, ob die konkrete Rolle des Unternehmens die Erbringung regulierter Zahlungsdienstleistungen umfasst. Darunter können – je nach inhaltlicher Ausgestaltung des Geschäftsmodells und tatsächlicher Rolle des Unternehmens – insbesondere das Ermöglichen oder Abwickeln von Zahlungsvorgängen, die Ausgabe oder der Transfer von E-Geld, grenzüberschreitende Geldtransfers oder Account- und Zahlungsinitiierungsfunktionen fallen. Digital Payment Token Services können demgegenüber Geschäftsmodelle erfassen, die den Handel, Transfer oder die Verwahrung digitaler Zahlungstoken beinhalten. Entscheidend ist nicht die Bezeichnung des Produkts, sondern die tatsächliche Funktion des Unternehmens im Geld- oder Tokenfluss. Das Lizenz- und Aufsichtsregime der **Monetary Authority of Singapore**

sollte daher vor der operativen Umsetzung geprüft werden. Aufgrund des Tätigkeitsumfangs gelten für Major Payment Institutions weitergehende Anforderungen, insbesondere zur Sicherung von Kundengeldern.

Cybersecurity sollte insbesondere bei Cloud-Outsourcing, konzernweiten Zugriffsrechten, Incident Response sowie kritischen oder infrastrukturell bedeutsamen Dienstleistungen als integrierter rechtlicher und vertraglicher Prüfpunkt behandelt werden.

Praxis-Check: Was Unternehmen prüfen sollten

- **Plattformdesign:** Rankings, Empfehlungen, Defaults, Delisting und Account-Sperrungen müssen transparent, konsistent und sachlich begründbar sein. Deutsche Prozesse und Best Practices können als Ausgangspunkt dienen, müssen aber an den jeweiligen Zielmarkt angepasst werden.
- **Geschäftsbedingungen:** Rate-Parity-Klauseln, Preisvorgaben, Koppelungen, Gebühren sowie Rabatt- und Kampagnenvorgaben sollten kartellrechtlich geprüft werden.
- **Datenstrategie:** Datenflüsse, Einwilligungsprozesse, Drittanbieterzugriffe, KI-Training und internationale Transfers müssen dokumentiert und rechtlich abgesichert sein.
- **Markteintrittsstruktur:** Gesellschaftsform, ausländische Beteiligung, Genehmigungen, BOI-Förderfähigkeit und sektorale Regulierung sind vor Aufnahme der Tätigkeit abzugleichen.
- **Governance:** Verantwortlichkeiten für Produktentscheidungen, Algorithmen, Datenschutz, Cybersecurity und regulatorische Kommunikation sollten klar zugewiesen werden.
- **Verträge und Durchsetzung:** Anwendbares Recht, Gerichtsstand, Schiedsvereinbarung, Vollstreckbarkeit und einstweiliger Rechtsschutz gehören in die frühzeitige Vertragsplanung.

Fazit

Thailand, Vietnam und Singapur verfolgen keinen einheitlichen DMA-Nachbau.

Gleichwohl werden digitale Geschäftsmodelle in allen drei Märkten zunehmend durch das Zusammenspiel von Wettbewerbs-, Datenschutz-, Sicherheits-, Verbraucher- und Sektorenregulierung geprägt. Einheitliche Konzernstandards oder für den deutschen Markt entwickelte Best Practices sind ein sinnvoller Ausgangspunkt, reichen aber nicht aus. Sie müssen an die jeweilige Plattformarchitektur, Datenverwendung, Sicherheitsorganisation, Marktstruktur und Zahlungsströme angepasst werden.

Für internationale Unternehmen liegt der entscheidende Hebel in einer integrierten Umsetzung: Wer Markteintritt, Produktdesign, Datenstrategie, Governance und Vertragsstruktur von Anfang an zusammenführt, reduziert regulatorische Risiken und schafft zugleich eine belastbarere Grundlage für digitales Wachstum in der APAC-Region.

Ihre Ansprechpartner:



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



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



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



Dr. Tino Haupt
Rechtsanwalt, Senior Associate
Ho-Chi-Minh-Stadt
+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
Rechtsanwältin | Associate
München
+49 89 23714 21668
sabrina.aurnhammer@luther-lawfirm.com



Leif Dustin Schneider
Rechtsanwalt, Counsel, Registiert als foreign lawyer (Vietnam)
Ho-Chi-Minh-Stadt
+84 (0)28 7300 1073
leif.schneider@luther-lawfirm.com



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



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



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

Stand: Oktober 2026