emerging tech decoded

LEX CONSULT EDITORIAL

BYTE/WISE

KEY HIGHLIGHTS

JUNE 2026

Artificial Intelligence

Regulatory Updates

- India Establishes AI Governance Architecture
- European Parliament Votes for AI Act Simplification Measures and Nudifier App Ban
- EU Finalizes Code of Practice for AI-Generated Content Marking and Labelling
- United States Issues Executive Order on Advanced AI Innovation and Security

Clause in Focus - Third-Party AI Models And AI Supply Chain Dependencies
Knowledge Corner - Placing on the Market vs Putting into Service
Compliance Snapshot - AI Procurement and Due Diligence

Privacy

Regulatory Updates

- EDPB Advances Common Templates for DPIAs and Personal Data Breach Notifications
- California Delete Act approaches August 2026 Implementation
- Council of Europe Publishes Draft Privacy Guidelines for Large Language Models
- EDPB Consults on Guidelines for Processing Personal Data for Scientific Research
- Indian Central Consumer Protection Authority (CCPA) Penalises PhysicsWallah and McAfee for Dark Patterns

Clause in Focus - Reasonable Security Safeguards and Technical & Organizational Measures
Knowledge Corner - Data Fiduciary vs Significant Data Fiduciary
Compliance Snapshot - Personal Data Inventory and Data Mapping

Digital Assets

Regulatory Updates

- Dubai VARA Introduces Enhanced Regulatory Framework for Crypto Margin Trading and Derivatives
- Australia Establishes Comprehensive Licensing Framework for Digital Asset Platforms
- South Korea Moves to Regulate Tokenized Assets and Stablecoins Under Existing Financial Laws
- UAE Capital Markets Authority Unveils Comprehensive Framework for Virtual Asset Activities

Clause in Focus - Custodial Ownership vs. User Entitlement Clauses
Knowledge Corner - Real-World Asset Tokenization: Bridging Traditional Finance and Crypto

Dark Patterns Check – Bait and Switch

BYTE/WISE

PART ONE

Ai

JUNE 2026

Ai / REGULATORY UPDATES

India Establishes AI Governance Architecture

In May 2026, India constituted the AI Governance and Economic Group (AIGEG) as an apex inter-ministerial body and central institutional mechanism for AI governance policy development and coordination. Shortly thereafter, the Government also constituted the Technology and Policy Expert Committee (TPEC), a standing expert advisory body tasked with providing specialized technical, policy and strategic expertise to support the AIGEG.

The AIGEG has been established to coordinate AI policy across ministries, departments, regulators and other stakeholders, while also examining AI risks, regulatory gaps, governance priorities and labor market impacts. The TPEC, in turn, is expected to provide expert inputs on emerging technologies, global regulatory developments, policy design and implementation challenges. Together, the two bodies create a formal governance architecture intended to support a coordinated and whole-of-government approach to AI governance in India.

The development represents an important institutional step in India's evolving AI governance framework. Rather than introducing a standalone AI law at this stage, the Government appears to be strengthening the institutional mechanisms through which future AI policy, governance measures and regulatory approaches may be developed.

European Parliament Votes for AI Act Simplification Measures and Nudifier App Ban

Earlier this week, the European Parliament voted in favor of amendments to the EU AI Act as part of the Digital Omnibus package. The measures seek to simplify implementation of the AI Act by reducing regulatory overlaps, providing greater legal certainty and adjusting implementation timelines while maintaining the legislation's core risk-based approach.

Under the proposal, obligations relating to stand-alone high-risk AI systems would apply from 2 December 2027, while obligations relating to AI systems embedded as safety components and covered by EU sectoral product safety legislation would apply from 2 August 2028. The package also postpones certain transparency requirements, including obligations relating to machine-readable labelling of AI-generated content, until 2 December 2026. In addition, it seeks to reduce regulatory overlap between the AI Act and sector-specific product safety legislation, narrow certain "safety component" classifications, and extend selected support measures to small mid-cap enterprises.

The Parliament also voted to prohibit so-called "nudifier" applications that use AI to generate sexually explicit or intimate content depicting identifiable individuals without their consent, as well as AI systems used to create child sexual abuse material. The measure reflects growing global concern around AI-enabled harms associated with deepfakes and synthetic media, particularly where AI is used to create realistic intimate imagery of individuals without consent.

EU Finalizes Code of Practice for AI-Generated Content Marking and Labelling

The European Commission published the final Code of Practice on Transparency of AI-Generated Content in June 2026, supporting implementation of the AI Act's obligations relating to marking and labelling AI-generated and manipulated content. The Code is intended to assist providers and deployers of generative AI systems in complying with the transparency obligations set out under Article 50 of the AI Act.

The Code provides practical guidance on marking and detecting AI-generated or manipulated content, labelling deepfakes, and identifying certain AI-generated text published to inform the public on matters of public interest. It distinguishes between the responsibilities of providers and deployers of AI systems, promotes both human-readable and machine-readable transparency measures, and provides guidance on the presentation of labels, disclosures and other indicators intended to improve transparency for end users.

While adherence to the Code is voluntary, the transparency obligations under Article 50 of the AI Act are currently expected to become applicable from 2 December 2026 following the European Parliament's vote in favor of postponing certain AI Act transparency requirements as part of the AI Act simplification package.

As highlighted in earlier ByteWise editions, China has already introduced more prescriptive labelling requirements for AI-generated content, while India has considered similar disclosure and labelling obligations under proposed AI-related amendments to the IT framework. These developments reflect an accelerating international effort to improve content provenance, authenticity and transparency, particularly in addressing the challenges posed by deepfakes and other forms of AI-generated or manipulated content.

United States Issues Executive Order on Advanced AI Innovation and Security

On 2 June 2026, the United States issued an Executive Order titled "Promoting Advanced Artificial Intelligence Innovation and Security". The Order focuses on the national security and cybersecurity implications of advanced AI systems while maintaining a pro-innovation regulatory approach.

A key feature of the Order is the development of a voluntary framework for engagement with developers of frontier AI models before broader release. The Order also directs government agencies to strengthen AI-enabled cybersecurity capabilities, protect American intellectual property and coordinate action against AI-enabled cyber threats. It is important to note that the approach does not impose mandatory licensing or pre-clearance requirements on AI developers. Instead, it seeks to provide the Government with greater visibility into emerging frontier AI capabilities and risks while enabling developers to continue releasing and deploying advanced AI systems without prior regulatory approval.

Ai / CLAUSE IN FOCUS

THIRD-PARTY AI MODELS AND AI SUPPLY CHAIN DEPENDENCIES

As enterprise AI tools increasingly rely on third-party AI models, cloud infrastructure, model-hosting providers, data-labelling vendors and system integrators, AI contracting is no longer limited to the immediate provider-deployer relationship. A vendor offering an AI solution may itself depend on multiple upstream providers for model access, training, inference, hosting, monitoring, security and support.

This creates risks similar to those associated with sub-processors in data protection arrangements, but with additional complexity. A change in an underlying foundation model, model provider, hosting environment or inference service may materially alter system behavior, outputs, capabilities, limitations or compliance characteristics without any change to the contracting party. As organizations increasingly rely on third-party AI models, visibility into material AI dependencies is becoming an important component of vendor governance, risk assessment and contractual oversight.

For this reason, AI agreements should increasingly address the use of third-party AI models and related dependencies as a specific contractual control point.

Draft Illustrative Clause

"The Provider shall disclose any material third-party AI model, model-hosting provider or other third-party dependency used in connection with the AI System and provide prior notice of any material change to such providers, models or services where such change may reasonably affect the Deployer's use of the AI System, compliance obligations, security posture or risk assessment"

Negotiation Points

Deployer / Customer

- Require disclosure of all material AI model providers and critical upstream dependencies.
- Seek prior notice, and in high-risk deployments, approval rights for replacement of model providers or hosting arrangements.
- Require flow-down obligations covering confidentiality, security, data protection, training restrictions, incident notification and regulatory cooperation.
- Ensure the Provider remains responsible for acts, omissions and failures of upstream AI service providers.

Provider / Vendor

- Limit disclosure obligations to material dependencies rather than all operational or infrastructure vendors.
- Preserve flexibility to change model providers, hosting arrangements or technical components without customer approval for routine or low-risk changes.
- Use prior notice rather than prior consent, except where changes materially affect security, compliance or agreed functionality.
- Limit responsibility for third-party providers to dependencies within the Provider's reasonable control.

Balanced drafting should give deployers sufficient visibility into the AI supply chain without requiring providers to disclose every technical component or seek approval for routine operational changes.

Ai / COMPLIANCE SNAPSHOT

AI Procurement and Due Diligence

As organizations increasingly adopt AI-enabled tools for productivity, customer engagement, analytics, software development and decision support, procurement decisions are becoming an important governance and risk management function. Many AI-related risks originate before deployment, at the stage where an AI system is selected, approved or onboarded.

Traditional vendor onboarding processes may not adequately address AI-specific considerations such as data usage practices, third-party AI dependencies, transparency, evolving functionality, regulatory obligations and contractual risk allocation. Accordingly, organizations should undertake appropriate due diligence before procuring or deploying AI systems.

Key Areas to Assess

- Intended use case and business purpose of the AI system.
- Provider governance, security controls, compliance commitments and transparency regarding system capabilities, limitations, intended use and known risks.
- Use of third-party AI models, hosted services or other material dependencies.
- Data usage, retention, training and privacy practices.
- Contractual protections covering confidentiality, security, intellectual property, incident notification, liability and regulatory compliance.

For many businesses, an initial procurement and due diligence review supported by existing legal, privacy, security and technology functions may be sufficient, provided it identifies the key risks, dependencies and governance considerations associated with the proposed AI system.

Quick Self-Check for Organizations

- Have we clearly identified and approved the intended AI use case?
- Have we assessed the provider and any material third-party AI dependencies?
- Have data usage, retention, training practices, security controls and contractual protections been reviewed and assessed for AI-specific risks?
- Have relevant legal, compliance, privacy, security and technology stakeholders completed their review?

AI procurement should be treated as a governance exercise rather than a purely commercial decision. A structured due diligence process helps organizations identify risks early, support informed decision-making and establish a stronger foundation for responsible AI deployment.

Ai

KNOWLEDGE
CORNER

Placing on the Market vs Putting into Service

The concepts of "placing on the market" and "putting into service" are fundamental to the operation of the EU AI Act. While the terms are often used interchangeably in commercial discussions, they serve distinct functions within the regulatory framework and determine when different obligations may arise.

Placing on the Market

The EU AI Act defines "placing on the market" as the first making available of an AI system or a general-purpose AI model on the Union market. This concept focuses on market availability. An AI system is placed on the market when it is first made available on the Union market in the course of a commercial activity, whether in return for payment or free of charge. The emphasis is on the point at which the system enters the market and becomes available to others.

For providers, placing an AI system on the market is a significant regulatory milestone, as many obligations relating to conformity assessment, technical documentation, risk management and compliance must generally be addressed before this stage is reached.

Putting into Service

The EU AI Act defines "putting into service" as the supply of an AI system for first use directly to the deployer or for the provider's own use in the Union for its intended purpose.

Unlike placing on the market, which focuses on availability, putting into service focuses on actual deployment and operational use. An AI system may therefore be put into service when it is first used for its intended purpose, including where an organization develops and deploys the system internally without making it available to third parties.

The concept ensures that regulatory obligations are not avoided simply because a system is used internally rather than supplied to customers or other organizations.

Why the Distinction Matters

Although both concepts are closely related, they address different stages in the AI lifecycle. Placing on the market concerns the first availability of an AI system or model within the EU market. Putting into service concerns the first operational use of the system for its intended purpose. In many commercial deployments, both events may occur around the same time. However, they need not coincide. An AI system may be placed on the market before it is deployed by a customer, while an internally developed AI system may be put into service without ever being placed on the market.

For example: A company develops an AI-powered customer support chatbot and makes it available to businesses across the European Union through a SaaS platform. The chatbot may be placed on the market when it is first made available to customers in the EU. The chatbot may then be put into service when a customer deploys and begins using it to respond to live customer queries.

Alternatively, a company that develops a similar AI chatbot solely for use by its own customer support team may put the system into service without ever placing it on the market.

Understanding the distinction helps organizations determine when obligations arise, how responsibilities are allocated, and whether a particular AI deployment falls within the scope of regulatory requirements. As AI systems increasingly move between development, testing, commercialization and internal deployment, these concepts provide important reference points for managing compliance throughout the AI lifecycle.

BYTE/WISE

PART TWO

PRIVACY

Privacy / REGULATORY UPDATES

EDPB Advances Common Templates for DPIAs and Personal Data Breach Notifications

The European Data Protection Board (EDPB) has continued its efforts to promote greater consistency in privacy compliance practices across the European Union through the publication of a Data Protection Impact Assessment (DPIA) template and a common Personal Data Breach notification template. The consultation on the DPIA template concluded in June 2026, while the breach notification template remains open for public consultation until August 5th, 2026.

The DPIA template is intended to assist organizations in structuring and documenting key elements of the assessment process, including descriptions of processing activities, risk identification, mitigation measures and residual risk assessments.

The breach notification template seeks to standardize the information submitted to supervisory authorities following a personal data breach, including details relating to affected individuals, categories of personal data involved, likely consequences of the incident and remediation measures undertaken.

These initiatives are expected to assist organizations in standardizing internal privacy governance processes, improving the quality and consistency of regulatory submissions, and reducing uncertainty around regulatory expectations. As organizations in India prepare for implementation of the DPDP framework, similar practical guidance and standardized templates from Indian regulators could significantly assist in driving consistent compliance practices across sectors.

California Delete Act approaches August 2026 Implementation

California's Delete Act, enacted in 2023, was designed to simplify the exercise of consumer deletion rights by establishing a centralized framework through which individuals can submit a single request directing registered data brokers to delete personal information relating to them. As part of this initiative, California launched the Data Broker Requests and Opt-Out Platform (DROP) in January 2026. Registered data brokers will be required to begin processing requests submitted through the platform from August 2026.

The framework significantly expands consumer control over data broker ecosystems by enabling individuals to exercise deletion rights through a single centralized request, rather than submitting separate requests to individual data brokers. For registered data brokers, this creates substantial operational obligations relating to verification, deletion workflows, recordkeeping and ongoing compliance with consumer requests. As implementation approaches, organizations operating within data broker and ad-tech ecosystems should assess their readiness for the new framework.

While distinct from the Consent Manager ecosystem contemplated under the DPDP Act, the framework demonstrates how regulators are increasingly exploring mechanisms to simplify the exercise of privacy-related choices, rights and requests.

BYTE/WISE

Council of Europe Publishes Draft Privacy Guidelines for Large Language Models

The Council of Europe has released draft guidelines addressing privacy and data protection considerations in the development and deployment of large language model ("LLM") systems. A notable feature of the draft is the proposed "Identify, Assess, Mitigate and Monitor" (IAMM) methodology, which provides a structured framework for managing privacy risks throughout the AI lifecycle:

Identify: Identify privacy and data protection risks arising from the design, development, deployment and use of LLM-based systems.

Assess: Evaluate the likelihood, severity and potential impact of identified risks on individuals and their rights.

Mitigate: Implement appropriate technical, organizational and governance measures to address identified risks.

Monitor: Continuously review and reassess risks as systems evolve and new use cases emerge.

The Guidelines also address a number of emerging AI-specific privacy issues, including risks that LLM systems may infer sensitive characteristics, behavioral traits or other personal information from prompts, interactions or generated outputs. The draft further discusses profiling risks, governance of multimodal systems that combine text, image and audio inputs, privacy risks associated with retrieval and memory functions, downstream uses of AI-generated outputs, and the allocation of accountability across developers, deployers and other actors involved in the AI supply chain.

EDPB Consults on Guidelines for Processing Personal Data for Scientific Research

The European Data Protection Board (EDPB) has adopted Guidelines 1/2026 on the processing of personal data for scientific research purposes under the GDPR for public consultation. The consultation, which remains open until 25 June 2026, seeks to provide greater clarity on how GDPR requirements apply to scientific research activities and the use of personal data in research settings.

The Guidelines clarify a number of issues that have historically created uncertainty under the GDPR, including the interpretation of "scientific research", the legal bases available for research-related processing, and the circumstances in which personal data collected for one purpose may be further processed for scientific research. A key clarification is that further processing for scientific research is generally presumed to be compatible with the original purpose of collection, although controllers must still identify an appropriate legal basis and implement suitable safeguards, including measures such as data minimization, pseudonymization, transparency and governance controls.

The EDPB also addresses the use of broad consent where specific research purposes cannot be fully identified at the time of collection, the distinction between anonymization and pseudonymization in research settings, allocation of responsibilities among multiple research actors, and the circumstances in which certain data subject rights may be restricted where exercising those rights would seriously impair or render impossible the research objective. The Guidelines also place significant emphasis on accountability measures and documenting safeguards throughout the research lifecycle.

BYTE/WISE

Indian Central Consumer Protection Authority (CCPA) Penalises PhysicsWallah and McAfee for Dark Patterns

In a landmark enforcement action, the Central Consumer Protection Authority ("CCPA") imposed penalties on PhysicsWallah Limited in June 2026 and McAfee Software India Private Limited in May 2026 for deploying dark patterns that impaired consumers' ability to make free and informed choices on their digital platforms. PhysicsWallah was fined INR 5 lakhs, while McAfee was fined INR 1 lakh, and both entities were directed to discontinue the identified practices and ensure compliance with the Guidelines for Prevention and Regulation of Dark Patterns, 2023.

In the PhysicsWallah case, the CCPA found that the company had automatically added a pre-selected donation to users' checkout baskets and used emotionally persuasive messaging to discourage users from opting out. The authority also observed that courses advertised as "free" were accessible only after users shared personal information, including their mobile numbers and email addresses. The CCPA characterized these practices as instances of "Basket Sneaking", "Confirm Shaming", and "Forced Action", holding that consumer consent cannot be presumed through pre-selected options and must instead be obtained through clear and affirmative action.

In McAfee's case, the CCPA examined the company's subscription renewal interface, where users were presented with the options "Renew Now" and "Accept Risk". The authority concluded that the interface used fear-based and manipulative design techniques that could pressure consumers into renewing subscriptions. The practices were classified as "Confirm Shaming", "Interface Interference", "Trick Question", and "Forced Action", and were found to constitute unfair trade practices under the Consumer Protection Act, 2019.

The orders demonstrate that the Dark Patterns Guidelines have moved beyond a compliance framework and into active enforcement. Businesses operating digital platforms should review their customer journeys, consent flows, subscription interfaces, and data collection practices to ensure that user choices are presented in a transparent and non-manipulative manner.

Privacy/ CLAUSE IN FOCUS

REASONABLE SECURITY SAFEGUARDS AND TECHNICAL & ORGANIZATIONAL MEASURES (TOMS)

While the DPDP Act and Rules do not prescribe a fixed list of security controls, Section 8 requires Data Fiduciaries to implement reasonable security safeguards to protect personal data and places corresponding obligations on Data Processors acting on their behalf. Similar obligations are reflected in Article 32 of the GDPR, which requires controllers and processors to implement appropriate technical and organisational measures having regard to the nature of processing and associated risks. In practice, many organisations continue to look to frameworks such as ISO 27001 as a useful benchmark for demonstrating security maturity, although certification itself is not mandatory and organisations may instead rely on alternative or compensating controls that achieve comparable security outcomes.

Contractual provisions relating to security safeguards are critical because they determine how security responsibilities are allocated between parties, establish minimum expectations for protection of personal data, and provide a basis for assessing compliance in the event of a security incident or regulatory investigation.

Draft Illustrative Clause

"The Processor shall implement and maintain appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed under this Agreement."

"The Processor shall periodically review and update such measures having regard to changes in technology, evolving threats, and the nature, scope, context, and purposes of processing."

Negotiation Points

Data Controller/Data Fiduciary

- Require baseline security measures to be documented, particularly where certifications, audit reports or independent assurance reports are not available.
- Prefer industry-standard certifications, independent audits or equivalent assurance mechanisms, with periodic reviews
- Require security obligations to flow down to sub-processors and other service providers handling personal data.
- Include contractual obligations requiring periodic review and updating of security measures.

Data Processor

- Retain flexibility to determine appropriate controls based on risk, operational requirements and evolving security practices.
- Align contractual commitments with existing security programmes, certifications, audits and industry standards where possible.
- Limit disclosure of sensitive security architecture and proprietary information.
- Avoid contractual commitments that impose security obligations materially exceeding those required by applicable law or recognised industry standards.

The objective is not to mandate a particular technology or certification, but to ensure that appropriate safeguards are maintained, periodically reviewed and capable of protecting personal data throughout the processing lifecycle.

BYTE/WISE

Privacy/ COMPLIANCE SNAPSHOT

Personal Data Inventory and Data Mapping

A personal data inventory is one of the foundational steps for implementing the DPDP Act. Without a clear understanding of what personal data is collected, where it is stored, why it is processed, who has access to it, and when it is deleted, organizations may struggle to operationalize notice, consent, rights handling, breach response, retention, vendor governance and security safeguards.

Under the DPDP framework, compliance is closely tied to purpose limitation, consent management, data principal rights, breach notification and accountability for processors. Each of these obligations depends on an organization being able to identify and trace personal data across systems, teams and third-party relationships. A data inventory is a living record of processing activities and data flows.

Key Areas to Map

- Categories of personal data collected, including customer, employee, vendor, user, child, financial, health, location or device-related data.
- Purpose of collection and processing, mapped to the relevant notice, consent or other basis for processing under the DPDP framework.
- Systems and repositories where personal data is stored, including applications, databases, cloud environments, logs, backups and archives.
- Internal teams or roles that access personal data and the purpose for which such access is granted.
- Data processors, vendors, sub-processors and other recipients with whom personal data is shared.

For many businesses, an initial inventory maintained through spreadsheets or existing governance tools may be sufficient, provided it identifies the critical elements necessary to ensure compliance.

Quick Self-Check for Organisations

- Do we know what categories of personal data are collected across business functions?
- Is each category of personal data linked to a defined purpose and notice?
- Do we know which systems, teams, vendors and processors handle personal data?
- Can we identify personal data quickly for rights requests, correction, erasure or breach assessment?

A data inventory helps identify gaps, reduce unnecessary data collection, support rights handling, improve incident response and demonstrate that processing activities are aligned with the purposes communicated to Data Principals.

Privacy

KNOWLEDGE
CORNER

Data Fiduciary vs Significant Data Fiduciary

Data Fiduciary vs Significant Data Fiduciary

Under the DPDP Act, a Data Fiduciary is any person who alone or in conjunction with others determines the purpose and means of processing personal data. Most obligations under the DPDP framework, including notice, consent, security safeguards, rights handling and breach notification, apply to all Data Fiduciaries regardless of size or industry.

However, the DPDP Act recognizes that certain organizations may present higher risks to individuals and society due to the scale, nature or impact of their processing activities. To address this, the Act creates a separate category known as the Significant Data Fiduciary (SDF), which may be designated by the Central Government based on factors such as the volume and sensitivity of personal data processed, risks to the rights of Data Principals, impact on the sovereignty and integrity of India, security of the State, electoral democracy and public order.

Additional Obligations for Significant Data Fiduciaries

While all Data Fiduciaries must comply with the DPDP Act, Significant Data Fiduciaries are subject to enhanced governance and accountability requirements. These may include:

- Appointment of a Data Protection Officer responsible for compliance and grievance handling.
- Appointment of an independent Data Auditor to evaluate compliance with the Act.
- Conducting periodic Data Protection Impact Assessments.
- Undertaking periodic audits and reviews of processing activities.

How Should Organizations Assess Their Risk?

A common question under the DPDP framework is whether an organization is likely to be designated as a Significant Data Fiduciary. At present, no SDF designations have been notified and the law does not prescribe specific thresholds based on user numbers, revenue, transaction volumes or categories of sensitive personal data. In the absence of formal thresholds, organizations may find it useful to assess factors commonly considered in risk-based privacy frameworks globally, including:

- The volume of personal data processed and the number of individuals affected.
- The nature and sensitivity of the data involved, including financial, health, location or behavioural data.
- The extent of profiling, analytics or automated decision-making activities.
- Whether the organization operates a large consumer-facing digital platform.
- The potential impact on individuals if the data were misused, compromised or processed unlawfully.

Financial services, fintech, healthcare, health-tech, large e-commerce platforms, social media platforms, digital advertising businesses and data aggregators may therefore warrant closer assessment than organizations processing limited volumes of personal data for internal business purposes.

Accordingly, organizations that may fall within this category should begin considering whether their existing governance structures, accountability mechanisms and risk management processes would be capable of meeting heightened regulatory expectations if designated in the future.

BYTE/WISE

PART THREE

DIGITAL ASSETS

JUNE 2026

BYTE/WISE

Dubai VARA Introduces Enhanced Regulatory Framework for Crypto Margin Trading and Derivatives

The Virtual Assets Regulatory Authority ("VARA") has issued Version 2.1 of its Exchange Services Rulebook ("Rulebook"), introducing enhanced governance, risk management, and operational requirements for licensed virtual asset service providers ("VASPs") offering exchange services in Dubai. The Rulebook became effective on March 31 and forms part of Dubai's broader strategy to strengthen oversight of the virtual asset sector while supporting innovation.

The Rulebook applies to all VARA-licensed VASPs engaged in exchange activities and includes specific provisions governing margin trading and exchange-traded derivatives ("ETDs"). These products typically involve greater levels of leverage and complexity and therefore require heightened regulatory oversight.

Under the revised framework, VASPs are required to implement robust risk management systems, establish appropriate margin monitoring procedures, and provide clear disclosures to clients regarding the risks associated with leveraged trading and derivative products. The objective is to enhance investor protection and promote responsible market participation.

A key feature of the Rulebook is the requirement that exchange transactions settle within 24 hours of execution. This measure is intended to reduce settlement risk, improve market efficiency, and strengthen confidence in the virtual asset trading ecosystem.

The Rulebook also imposes market conduct obligations on VASPs, including the implementation of market-surveillance mechanisms designed to detect suspicious trading activity, market manipulation, and other forms of misconduct. In addition, VASPs must adopt internal codes of conduct and compliance procedures to ensure fair and orderly market operations.

Importantly, the Rulebook grants VARA authority to intervene where necessary to safeguard market stability, including the power to suspend trading activities and modify margin requirements in response to market conditions.

The introduction of the Rulebook represents a significant milestone in Dubai's virtual asset regulatory landscape. By establishing a comprehensive framework for crypto margin trading and derivatives, VARA continues to position Dubai as a leading jurisdiction for digital asset businesses while promoting transparency, market integrity, and investor protection.

Australia Establishes Comprehensive Licensing Framework for Digital Asset Platforms

Australia has taken a significant step toward regulating the digital asset sector following the passage of the Corporations Amendment (Digital Assets Framework) Act 2026 ("DAF Act"). The legislation, introduces a dedicated regulatory framework for digital asset platforms and tokenised custody platforms under Australia's financial services regime. The new framework is scheduled to commence on 9 April 2027, providing industry participants with an 18-month transition period to achieve compliance.

For the purposes of the DAF Act, a "Digital Asset Platform" ("DAP") broadly refers to a platform that holds or manages digital tokens on behalf of clients, while a "Tokenised Custody Platform" ("TCP") refers to a platform that issues digital tokens representing rights in underlying assets and acts as custodian of those assets. The legislation also introduces the concept of "Digital Tokens" as a distinct asset category within Australia's regulatory framework.

A key feature of the DAF Act is the requirement for covered DAPs and TCPs to obtain an Australian Financial Services Licence ("AFSL") and comply with obligations comparable to those applicable to traditional financial service providers. These obligations include asset safeguarding requirements, disclosure standards, consumer protection measures, and ongoing compliance obligations designed to promote market integrity and investor confidence.

The framework also grants the Australian Securities and Investments Commission ("ASIC") broad supervisory and enforcement powers, including authority to issue regulatory guidance, monitor compliance, and take enforcement action against non-compliant operators. The legislation further includes targeted exemptions for certain low-risk activities while enabling regulators to respond to future developments in the digital asset sector.

The DAF Act represents one of Australia's most significant crypto regulatory reforms to date. By bringing crypto exchanges and custody providers within the established financial services framework, Australia aims to enhance consumer protection, increase regulatory certainty, and support the responsible growth of its digital asset industry.

South Korea Moves to Regulate Tokenized Assets and Stablecoins Under Existing Financial Laws

South Korea has taken a significant step toward integrating digital assets into its mainstream financial system following a proposal by the ruling Democratic Party to incorporate tokenized real-world assets ("RWAs") and stablecoins into the country's proposed Digital Asset Basic Act ("DABA"). The proposal seeks to regulate these assets within existing financial legislation rather than creating an entirely separate regulatory framework.

Under the proposal, issuers of tokenized RWAs would be required to place the underlying assets into managed trusts in accordance with South Korea's Capital Markets Act. This requirement is intended to ensure that the assets backing RWA tokens remain legally segregated, properly safeguarded, and available to support investor claims. Additional operational requirements are expected to be introduced through future presidential decrees.

The proposed framework also introduces a comprehensive regime for stablecoins. For the purposes of the DABA, stablecoins would be classified as "payment instruments" under the Foreign Exchange Transactions Act, bringing issuers and operators under the supervision of foreign exchange authorities. While larger transactions would remain subject to reporting and compliance obligations, certain low-value stablecoin payments for goods and services would be exempt from foreign exchange reporting requirements.

Notably, the proposal prohibits stablecoin issuers from offering returns or yield on idle customer balances, a measure designed to distinguish payment-focused stablecoins from investment products and mitigate potential financial stability risks. The proposal also directs the Financial Services Commission ("FSC") to develop technical standards for interoperability, enabling stablecoins issued on different blockchain networks to operate seamlessly within the broader digital asset ecosystem.

In addition, the DABA contemplates the creation of a unified disclosure framework for digital assets, aimed at improving transparency, investor protection, and market integrity. The proposal reflects South Korea's broader objective of establishing a comprehensive regulatory framework for digital assets while supporting innovation in tokenization, digital payments, and blockchain-based financial services. If enacted, the legislation could position South Korea as one of Asia's leading jurisdictions for regulated digital asset activity.

UAE Capital Markets Authority Unveils Comprehensive Framework for Virtual Asset Activities

The UAE Capital Markets Authority ("CMA"), formerly known as the Securities and Commodities Authority ("SCA"), has introduced a new regulatory framework for virtual asset activities in onshore UAE (the "New Framework"), marking a significant development in the country's digital asset regulatory landscape. The New Framework reflects the UAE's continued commitment to establishing a robust and innovation-friendly environment for virtual asset businesses while enhancing regulatory oversight and investor protection.

The New Framework expands the scope of regulated virtual asset activities and introduces a more comprehensive licensing and supervisory regime for market participants operating in the digital asset sector. The reforms are intended to align the UAE's regulatory approach with the increasing sophistication of virtual asset markets and the growing institutional interest in blockchain-based financial products.

One of the most notable features of the New Framework is the introduction of a dedicated Alternative Trading System ("ATS") module. The ATS framework applies not only to virtual asset trading facilities but also to conventional multilateral trading facilities ("MTFs") for securities and MTFs dedicated to tokenized securities. This development highlights the regulator's recognition of the growing convergence between traditional capital markets and digital asset markets.

By expressly addressing tokenized securities trading platforms, the CMA has created a regulatory pathway for the development of blockchain-based capital market infrastructure, which could support the issuance, trading, and settlement of tokenized financial instruments in the future.

The New Framework replaces the legacy virtual asset regulations previously administered by the SCA prior to its reconstitution as the CMA. To facilitate an orderly transition, existing licensees operating under the legacy framework have been granted a one-year transition period to comply with the revised requirements.

The CMA has also clarified the position of pending license applicants. Applicants that have already received initial approval under the legacy regime may continue their licensing process under the New Framework. However, applicants that have not yet obtained initial approval will be required to amend their applications to align with the revised regulatory requirements or withdraw their applications altogether.

The introduction of the New Framework further strengthens the UAE's position as a leading digital asset jurisdiction. By modernizing its regulatory architecture and addressing emerging business models such as tokenized securities and virtual asset trading platforms, the CMA is seeking to promote innovation while maintaining high standards of market integrity, transparency, and investor protection.

Digital Assets / CLAUSE IN FOCUS

CUSTODIAL OWNERSHIP VS. USER ENTITLEMENT CLAUSES

As digital asset markets mature, one of the most consequential yet often overlooked contractual provisions is the custody clause governing the legal relationship between an exchange and its users. While users generally assume that cryptocurrencies reflected in their exchange accounts belong to them in the same manner that funds in a bank account are held for their benefit, exchange terms increasingly adopt a different legal construct. Rather than recognizing users as direct owners of the underlying digital assets, many platforms characterize the user's interest as a contractual claim against the exchange for an equivalent quantity and type of digital asset.

Balanced drafting should carefully distinguish between operational custody arrangements and legal ownership rights. While exchanges require flexibility to maintain scalable custody models, users increasingly expect contractual certainty regarding the treatment of their assets during extraordinary events such as insolvencies, enforcement actions, or cybersecurity incidents.

Draft Illustrative Clause

"The User acknowledges and agrees that Digital Assets maintained through the Platform may be held in omnibus wallets together with Digital Assets attributable to other users of the Platform and, where permitted by applicable law, assets maintained by the Platform for operational purposes. The User's account balance shall represent a contractual entitlement against the Platform to the quantity and type of Digital Assets recorded in the User's account from time to time and shall not constitute ownership of, or any proprietary interest in, any specific Digital Asset, wallet address, private key, or blockchain account maintained by the Platform. Except to the extent expressly required under applicable law or agreed otherwise inwriting, no trust, fiduciary, custodial, or similar relationship shall be deemed to arise solely by virtue of the User maintaining Digital Assets through the Platform. The Platform shall maintain books and records sufficient to identify and attribute Digital Asset balances to individual users and shall implement custody and safeguarding measures consistent with applicable legal and regulatory requirements."

Negotiation Points

Exchange

- Preserve omnibus custody arrangements to facilitate operational efficiency and liquidity management.
- Retain the ability to pool customer assets with assets attributable to other users for operational and settlement purposes.
- Clarify that customer balances represent contractual entitlements rather than ownership of specifically identifiable blockchain assets.
- Limit liability arising from insolvency, blockchain forks, network disruptions, or custodial failures beyond expressly assumed obligations.

User / Institutional Customer

- Seek segregation of customer assets from proprietary assets of the platform.
- Require express recognition of beneficial ownership over digital assets credited to the customer account.
- Request trust-based or bankruptcy-remote custody arrangements where feasible.
- Obtain transparency regarding wallet structures, custody providers, and safeguarding practices.
- Ensure contractual protections against rehypothecation, lending, staking, or other uses of customer assets without consent.
- Seek priority treatment and enhanced recovery rights in insolvency or restructuring scenarios.

Digital Assets

KNOWLEDGE
CORNER

Real-World Asset (RWA) Tokenization: Bridging Traditional Finance and Crypto

BYTE/WISE

The cryptocurrency industry is evolving beyond digital payments and speculative trading. One of the most significant developments shaping the sector today is the tokenization of real-world assets (“RWAs”), a process that is transforming how traditional assets are owned, traded, and managed through blockchain technology.

For the purposes of this article, "Real-World Assets" or "RWAs" refer to tangible assets and traditional financial instruments, including real estate, bonds, commodities, and equities. "Tokenization" refers to the process of representing ownership rights or economic interests in such assets through blockchain-based digital tokens ("Tokens").

By converting ownership interests into Tokens, asset issuers can facilitate fractional ownership, enabling investors to gain exposure to high-value assets with significantly lower capital commitments. Blockchain technology and smart contracts further streamline transactions by automating settlement processes, reducing administrative costs, and enhancing transparency.

RWA tokenization is attracting considerable attention because it has the potential to bridge traditional finance ("TradFi") and decentralized finance ("DeFi"). While the global financial market represents hundreds of trillions of dollars in value, the cryptocurrency market remains comparatively small. Tokenization creates a pathway for bringing traditional assets on-chain, thereby unlocking new liquidity and investment opportunities.

The key benefits of RWA tokenization include:

- Fractional Ownership: Investors can acquire smaller interests in high-value assets.
- Enhanced Liquidity: Traditionally illiquid assets may become easier to trade through secondary markets.
- Operational Efficiency: Smart contracts can automate transfers, distributions, and compliance functions.
- Transparency: Blockchain-based records provide greater visibility and auditability of transactions.

Institutional participation is also accelerating. Leading asset managers and financial institutions are increasingly exploring tokenized investment products and blockchain-based fund structures. This trend reflects growing confidence in blockchain infrastructure and its potential to modernize capital markets.

At the same time, DeFi platforms are integrating tokenized RWAs to support lending, borrowing, and yield-generation activities. By introducing assets backed by real economic value, the sector is moving toward more sustainable and diversified financial products.

Despite these opportunities, regulatory and compliance challenges remain. Issues relating to securities laws, investor protection, custody, and cross-border transfers continue to require careful consideration. Clear and consistent regulatory frameworks will be essential for long-term growth.

As blockchain adoption continues to expand, RWA tokenization is positioned to become a key driver of the next phase of crypto innovation. By connecting digital infrastructure with tangible economic assets, tokenization has the potential to redefine global finance and create a more accessible and efficient investment ecosystem.

BYTE/WISE

PART FOUR

DARK PATTERNS

JUNE 2026

BYTE/WISE

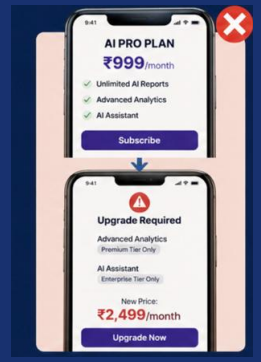
BAIT AND SWITCH

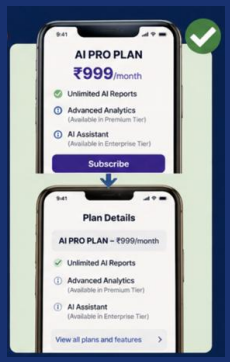
The Guidelines for Prevention and Regulation of Dark Patterns, 2023 define "Bait and Switch" as a practice whereby a consumer is attracted through an offer, advertisement or representation of a particular product, service, price or benefit, but is subsequently presented with a materially different offering.

Common manifestations include:

- ❌ Advertising a product at an attractive price that is unavailable or out of stock when the consumer attempts to purchase it
- ❌ Promoting a service plan with specific features that are only available through a more expensive tier
- ❌ Highlighting a discounted offer while steering consumers toward higher-priced alternatives during checkout
- ❌ Marketing a "free" or "basic" version of a product that lacks the functionality prominently advertised
- ❌ Displaying search results or recommendations that appear to match the consumer's selection but redirect to different products or plans

Bait and switch practices are problematic because consumers make purchasing decisions based on initial representations. Where the advertised offering differs materially from what is ultimately available, consumer choice may be distorted and comparisons between competing products may become misleading.





Better practice

- ✅ Ensure advertisements accurately reflect products, services and features that are genuinely available
- ✅ Clearly disclose eligibility criteria, feature limitations and availability conditions before consumers begin the purchase process
- ✅ Present alternative products or upgrades as optional choices rather than substitutes for the advertised offering
- ✅ Maintain consistency between promotional materials, product descriptions and checkout journeys
- ✅ Review marketing and onboarding flows to ensure consumers receive the offering they reasonably expect based on the advertisement

Tip for businesses

Review marketing campaigns, landing pages, app stores, product comparison pages and subscription flows to identify instances where consumers may be attracted by one offering but ultimately presented with another. Businesses should ensure that advertisements, product descriptions and pricing information remain accurate and consistent throughout the customer journey.

BYTE/WISE

COMING SOON

JULY ISSUE

ISSUE EDITORS

Partner: Naresh Pareek

Consultant: Shravan Kalluri

CONTRIBUTORS

Abhishek Nair

Jash Doshi

PUBLISHING SUPPORT

Vivek Yadav

309-10 Madhava,
C5, E Block, BKC,
Bandra East,
Mumbai 400 051