emerging tech decoded

LEX CONSULT EDITORIAL

BYTE/WISE

KEY HIGHLIGHTS

JULY 2026

Artificial Intelligence

Regulatory Updates

- China Regulates AI Companion Services
- US States Expand AI Chatbot Regulation
- Supreme Court of India Releases Draft Regulations for Use of Artificial Intelligence in Courts

Clause in Focus – Model Deprecation & Sunset Obligations

Knowledge Corner - Synthetic Data

Compliance Snapshot - Record-Keeping for AI-Generated Outputs

Privacy

Regulatory Updates

- EDPB Adopts Guidance on Anonymization and Web Scraping for Generative AI
- US Supreme Court Decision Renews Debate over EU-US Data Transfers
- India Initiates Process for Constituting the Data Protection Board
- EDPB Finalizes Blockchain Data Protection Guidelines

Clause in Focus - Confidentiality and Personnel Access Controls

Knowledge Corner - Controller vs Joint Controller

Compliance Snapshot - Purpose Mapping

Digital Assets

Regulatory Updates

- EU Plans to Review MiCA Rules to Include Non-EU Stablecoin Issuers
- ASIC Extends Licensing Relief for Digital Asset Businesses in Australia
- RBI Reaffirms Its Stand on Cryptocurrency: No Legal Status Yet
- Hong Kong Completes Its Crypto Regulatory Framework

Clause in Focus - Token Delisting Clause

Knowledge Corner - Decentralized Finance (DeFi): The Next Frontier in Digital Assets

Dark Patterns Check– Basket Sneaking

BYTE/WISE

PART ONE

Ai

JULY 2026

Ai / REGULATORY UPDATES

China Regulates AI Companion Services

China has recently introduced a comprehensive regulatory framework governing AI companion and anthropomorphic interaction services, moving beyond general-purpose AI regulation to address AI systems designed to simulate human relationships. On April 10, 2026, the Cyberspace Administration of China, together with the NDRC, MIIT, MPS and SAMR, jointly issued the Interim Measures for the Administration of AI Anthropomorphic Interaction Services ("Measures"), which took effect on July 15, 2026. These Measures apply specifically to services that simulate human personality, thought patterns and communication styles to provide ongoing emotional engagement, including AI companions, virtual partners and emotional care chatbots. The Measures impose layered compliance obligations aimed at addressing the distinctive risks associated with anthropomorphic AI.

Key requirements include:

- Governance and risk management: establishing safety-management systems throughout the service lifecycle, including algorithm review, technology ethics, content management, cybersecurity, personal information protection and emergency response mechanisms;

- Protection against emotional dependency: implementing AI identity disclosures, reminders following prolonged interaction, and safeguards to discourage unhealthy emotional reliance or the replacement of real-world interpersonal relationships;

- Enhanced protections for minors: implementing age verification, obtaining guardian consent where required, restricting certain anthropomorphic features, and providing supervised "minor mode" settings;

- Interaction data governance: protecting users' interaction data, providing options to copy and delete interaction histories, and obtaining separate consent before using sensitive interaction data for model training; and

Even before the Measures took effect, several major AI platforms reportedly modified or withdrew companion-style features in anticipation of the new regulatory requirements, illustrating the practical impact of the framework on product design and deployment. Further, these Measures reflect growing regulatory concern regarding AI systems capable of forming sustained emotional relationships with users, particularly where such interactions may affect vulnerable individuals or minors.

BYTE/WISE

US States Expand AI Chatbot Regulation

As noted in an earlier edition of ByteWise, New York and California introduced the first dedicated laws regulating AI companion chatbots. Since then, state regulation has expanded rapidly. In the absence of a comprehensive federal framework, eleven US states had enacted chatbot legislation by June 2026, with additional states considering similar measures. While these laws pursue common policy objectives, they differ in the categories of chatbots they regulate, with some applying broadly to conversational AI systems and others focusing specifically on AI companion chatbots designed to simulate sustained human relationships.

Although the laws differ in scope, they share a common regulatory structure. Common requirements include transparency obligations informing users that they are interacting with an AI system, safeguards addressing suicide, self-harm and other harmful interactions, enhanced protections for minors, and measures designed to limit emotionally manipulative or dependency-forming interactions. However, these State laws also diverge in important respects.

New York and California regulate AI companion chatbots capable of sustaining ongoing human-like relationships, whereas states such as Colorado, Idaho, Iowa and Nebraska have adopted broader legislation covering conversational AI services more generally. At the federal level, the proposed Guidelines for User Age-verification and Responsible Dialogue (GUARD) Act, which has been approved by the Senate Judiciary Committee but has not yet been enacted, would introduce nationwide age-verification requirements, prohibit minors from accessing AI companions, require AI chatbots to disclose that users are interacting with artificial intelligence, and establish criminal penalties for certain AI companion interactions that encourage suicide, self-harm or violence involving minors.

Supreme Court of India Releases Draft Regulations for Use of Artificial Intelligence in Courts

The Supreme Court of India's AI Committee published the Draft Regulations for Use of Artificial Intelligence in Courts, 2026 for public consultation, proposing a comprehensive governance framework for the responsible use of AI across the Indian judiciary.

Key highlights include:

- Human oversight and judicial accountability: AI cannot determine judicial outcomes or replace judicial reasoning and discretion. Judicial officers remain responsible for independently reviewing and verifying AI-assisted outputs before relying on them.
- Permitted uses of AI: AI may be used to support administrative and assistive functions, including legal research, translation, transcription, summarization, drafting assistance and case management, subject to appropriate human review.
- Privacy and confidentiality: The draft emphasizes appropriate safeguards for judicial records and personal data, including security measures to protect confidential court information processed through AI systems.
- Disclosure and verification: Legal practitioners using AI to prepare pleadings or other submissions may be required to disclose such use and remain responsible for verifying the accuracy and correctness of AI-assisted content before filing.

The draft Regulations seek to facilitate the use of AI in judicial and administrative functions while reaffirming that AI must remain an assistive tool and cannot replace human judicial decision-making.

Ai / CLAUSE IN FOCUS

MODEL DEPRECATION & SUNSET OBLIGATIONS

AI models are not static products. Providers routinely retire, replace, or materially retrain the models underlying their services, whether to improve performance, retire costly infrastructure, or respond to safety and regulatory findings. For a provider, deprecation is a normal part of the product lifecycle. For a customer that has integrated a specific model version into a workflow, product, or regulated process, however, deprecation can mean a sudden change in outputs, a break in downstream compatibility, or the loss of a system that has already been validated, tested, or approved for a specific use.

Unlike the Model Updates clause discussed in earlier Bytewise editions, which addresses incremental changes to a model that remains in service, deprecation and sunset provisions address the harder case: the end of a model's availability altogether, and what notice, transition support, and continuity obligations apply before that happens.

Draft Illustrative Clause

"The Provider may discontinue or withdraw availability of any version of the AI System ("Deprecation") upon not less than [x] days' prior written notice to the Customer, except where earlier discontinuation is required for legal, regulatory, security or safety reasons, in which case the Provider shall provide such notice as is reasonably practicable in the circumstances."

"During the notice period referred to above (the "Sunset Period"), the Provider shall maintain availability of the deprecated version substantially in accordance with the terms of this Agreement, and shall not degrade its performance, functionality, or support save as necessary to give effect to the Deprecation."

"Where the Customer is unable to complete migration to a successor model within the Sunset Period despite reasonable efforts, the parties shall discuss in good faith an extension of the Sunset Period or alternative transitional arrangements, provided that the Provider shall not be obliged to maintain a deprecated version beyond [x] additional days."

Negotiation Points

BYTE/WISE

Deployer / Customer

- Seek longer, tiered notice periods calibrated to the criticality of the use case, with extended notice for models embedded in regulated or safety-relevant workflows.
- Require the deprecation notice to identify the retirement date, any applicable service limitations during the Sunset Period and the Provider's recommended successor model.
- Negotiate a right to extend the Sunset Period, or to receive credits or fee adjustments, where migration cannot reasonably be completed in time.
- Where the Customer's own product has been certified, audited, or regulatory-approved by reference to a specific model version, seek a longer minimum sunset commitment tied to that dependency.

Provider / Vendor

- Preserve the ability to shorten or bypass notice periods where deprecation is driven by legal, safety, or security requirements.
- Cap the maximum duration of any extended Sunset Period, to avoid indefinite obligations to maintain legacy infrastructure.
- Limit transition assistance to the provision of information, rather than active migration support, unless separately scoped and priced.
- Avoid commitments to maintain functional, performance or output parity between deprecated and successor models

Because deprecation shifts risk from the provider's product roadmap onto the customer's operational and compliance timeline, well-drafted sunset clauses function as a form of risk-sharing: they do not prevent a provider from evolving its models, but they ensure that the cost of that evolution, in notice, information, and transition time, is allocated deliberately rather than left to fall entirely on the party least able to control it.

BYTE/WISE

Ai / COMPLIANCE SNAPSHOT

Record-Keeping for AI-Generated Outputs

As organizations increasingly rely on AI systems to support decisions, communications and business processes, risks arise not only from how outputs are generated, but from whether organizations can later explain what was produced, on what basis, and by which version of a system. Appropriate record-keeping enables organizations to demonstrate accountability, investigate incidents, respond to regulatory or customer enquiries, and support internal audits where AI systems influence business outcomes.

What Record-Keeping Should Cover

- Output Records: Material outputs generated by AI systems, particularly those informing decisions or customer-facing communications, should be retained for a period sufficient to meet regulatory, contractual, and dispute-resolution needs.
- Input and Prompt Documentation: Where appropriate to the use case, retain sufficient information regarding the prompts, inputs or source data that materially influenced an output to support traceability, investigation or audit.
- Model Version Tracking: Maintain records identifying the AI system or model version used to generate an output, particularly where models are updated, replaced or retired over time.
- Human Review Records: Where human review, approval or intervention forms part of the organization's governance process, maintain records of that review, including any material modifications made before the output is relied upon.
- Access and Usage Logs: Maintain appropriate records of access to AI systems and their outputs, particularly for sensitive or high-impact use cases.

In addition to the above, the extent of record-keeping should be proportionate to the nature and risk of the AI use case. Systems supporting legal, financial, employment, healthcare or other high-impact decisions typically warrant more comprehensive documentation than low-risk or purely assistive applications.

Quick Self-Check for Organizations

- Can we identify and retrieve the records necessary to explain how a material AI-generated output was produced?
- Do our records identify which model version generated a given output, including when that version has since been updated or retired?
- Where outputs are reviewed by a human, is that review documented in a way that could be produced on request?
- Are retention periods for AI-generated outputs aligned with applicable regulatory and contractual requirements?
- Are our record-keeping practices proportionate to the level of risk presented by the relevant AI use case?

Organizations should ensure AI-generated outputs remain traceable through robust documentation integrated into governance frameworks, including retention policies, links between outputs, inputs, and model versions, and records of human review across functions.

Ai

KNOWLEDGE
CORNER

Synthetic Data

Synthetic data refers to data that is artificially generated rather than directly collected from real individuals or events. The European Commission and the U.S. Trade and Technology Council's Terminology and Taxonomy for Artificial Intelligence defines synthetic data as:

"Synthetic data is data artificially generated by a computational process rather than being captured by sensory apparatus or manually created by humans. Synthetic data is often produced by a model trained to reproduce the characteristics and structure of its training data, aiming for similar distribution."

Depending on the nature and intended use of the original data, synthetic data may be generated using statistical models, AI systems or computer simulations that reproduce statistical patterns, generate new records with similar characteristics or simulate realistic artificial scenarios. Some methods also incorporate privacy-enhancing techniques, such as differential privacy, which introduces carefully calibrated statistical noise to limit the influence of any individual record while preserving the overall usefulness of the dataset.

The growing use of foundation models, increasing privacy obligations and the limited availability of high-quality real-world datasets have significantly increased interest in synthetic data as a means of supporting responsible AI development. Synthetic data has emerged as an important tool for developing, testing and improving AI systems, particularly where access to real-world data is constrained by privacy, confidentiality or commercial considerations. It enables organizations to supplement limited datasets during model development, evaluate AI systems without exposing personal information, simulate rare but critical events such as financial fraud, cybersecurity incidents or uncommon medical conditions, identify and mitigate bias by creating more balanced datasets, and support privacy-preserving AI development while retaining the statistical characteristics necessary for meaningful analysis.

Although synthetic data is not itself subject to a dedicated regulatory framework, it is increasingly recognized within AI and data governance. While the EU AI Act does not distinguish between real and synthetic datasets, Article 10 requires providers of high-risk AI systems to implement appropriate data governance and data management practices for training, validation and testing datasets. Separately, Recital 7 of the EU Data Governance Act identifies the use of synthetic data as one of several techniques, including anonymization and differential privacy, that can contribute to more privacy-friendly processing of data and facilitate the safe reuse of protected data.

Singapore's Personal Data Protection Commission (PDPC) has published a Proposed Guide on Synthetic Data Generation, one of the most comprehensive official guidance documents dedicated to synthetic data. The Guide emphasizes that synthetic data is not inherently privacy-preserving and recommends governance measures covering purpose definition, generation methodology, utility evaluation, privacy-risk assessment, documentation, and appropriate contractual, organizational and technical safeguards to manage residual re-identification risks. However, it should not be treated as automatically anonymous. As discussed in an earlier edition of ByteWise, anonymized data is derived from real personal data that has been processed to prevent the identification of individuals, while pseudonymized data remains personal data because individuals can still be re-identified using additional information. Unlike anonymized or pseudonymized data, synthetic data is not created by modifying existing records. Depending on the generation method and the similarity to the source data, synthetic datasets may still present disclosure or re-identification risks, making appropriate testing and governance essential.

BYTE/WISE

PART TWO

PRIVACY

Privacy / REGULATORY UPDATES

EDPB Adopts Guidance on Anonymization and Web Scraping for Generative AI

At its July 2026 plenary meeting, the European Data Protection Board (EDPB) adopted draft guidelines for public consultation on anonymization and web scraping in the context of generative AI, with the consultation remaining open until 30 October 2026. The two draft guidelines address issues of increasing significance for organizations developing and deploying generative AI systems.

Key highlights – Draft Guidelines on Anonymization

- Data will cease to constitute personal data only where individuals are no longer identifiable, taking into account the means of re-identification reasonably likely to be available to the person or organization receiving the data.

- Organizations should assess anonymization against three principal risks: whether an individual can be singled out, linked with other datasets, or have additional information inferred about them.

- Removing direct identifiers alone is unlikely to be sufficient. Controllers should evaluate anonymization techniques in light of the specific context, available auxiliary information and residual re-identification risks.

Key highlights – Draft Guidelines on Web Scraping for Generative AI

- The public availability of personal data does not remove organizations' obligations under the GDPR. Controllers scraping online content remain responsible for identifying an appropriate lawful basis and complying with the GDPR's core principles.

- The draft guidelines recommend collecting data from reliable sources, validating scraped information before using it for AI training, and recording the timestamp of collected data where appropriate to support data quality and accountability.

- Organizations should implement appropriate safeguards where web-scraped datasets may contain special-category personal data or information relating to vulnerable individuals, and should assess whether the scale and context of scraping affect individuals' reasonable expectations.

For organizations developing, fine-tuning or procuring generative AI systems, the draft guidelines provide practical direction on two foundational aspects of AI governance: when training data may genuinely be regarded as anonymous, and how publicly available personal data may be collected and used consistently with the GDPR.

US Supreme Court Decision Renews Debate over EU-US Data Transfers

A recent decision of the United States Supreme Court in *Trump v. Slaughter* has reignited debate regarding the long-term stability of the EU-US Data Privacy Framework (DPF). The judgment held that statutory protections limiting the President's power to remove Federal Trade Commission (FTC) commissioners are unconstitutional, prompting questions about one of the institutional safeguards considered by the European Commission when adopting its adequacy decision.

European privacy advocacy groups have argued that the ruling undermines the independence of the FTC, a key supervisory authority under the commercial oversight component of the DPF, and have called on the European Commission to withdraw its adequacy decision. Other commentators have noted that the judgment does not directly affect the Data Protection Review Court established under Executive Order 14086 and therefore does not automatically invalidate the Framework, particularly as the redress mechanism operates under a separate legal framework.

At present, the EU-US Data Privacy Framework remains fully valid, and organisations may continue relying on it for transfers of personal data to participating US organisations. However, businesses should continue monitoring developments, particularly any response from the European Commission or the European Data Protection Board, as well as any future legal challenges concerning the Framework.

India Initiates Process for Constituting the Data Protection Board

The Ministry of Electronics and Information Technology has initiated the process of constituting the Data Protection Board of India by inviting applications for the positions of Chairperson and Members. The deadline for submitting applications expired on 6 July 2026.

The Board, under the Digital Personal Data Protection Act, 2023, will serve as India's principal adjudicatory authority for matters relating to non-compliance with the Act. Its functions include conducting inquiries, issuing directions and imposing financial penalties once operational.

While the recruitment process represents an important institutional milestone, the Board is not yet operational and appointments remain pending. Organizations should nevertheless view the development as another indication that India's privacy enforcement framework continues to move from legislation towards implementation.

BYTE/WISE

EDPB Finalizes Blockchain Data Protection Guidelines

The European Data Protection Board (EDPB) has adopted the final version of its Guidelines on the Processing of Personal Data through Blockchain Technologies following public consultation. The guidelines provide practical direction on applying the GDPR to blockchain deployments, addressing key governance, accountability and data protection challenges arising from distributed ledger technologies.

Key highlights

- Assess whether blockchain is necessary: Organizations should first determine whether a blockchain solution is appropriate for the intended processing or whether the objective can be achieved using less privacy-intrusive technologies.

- Minimize on-chain personal data: The guidelines reiterate that personal data should, wherever possible, be stored off-chain, with only the minimum information necessary recorded on the ledger. Hashes, public keys and wallet addresses may themselves constitute personal data depending on the circumstances.

- Clarify governance and accountability: Organizations should identify the relevant controllers and processors before deployment, recognizing that decentralized architectures do not automatically eliminate GDPR responsibilities. Different blockchain architectures may lead to different allocations of responsibility.

- Address data subject rights by design. The practical immutability of blockchain does not remove obligations relating to data minimization, storage limitation, rectification and erasure. Organizations should design governance and technical measures that enable compliance with these principles as far as possible.

For organizations exploring blockchain for digital identity, supply-chain management, tokenization or financial services, the guidelines reinforce that GDPR compliance depends not on the technology itself, but on appropriate system design, governance arrangements and privacy-by-design measures. Beyond the GDPR, the guidelines emphasize a broader principle that the adoption of blockchain does not displace established privacy principles, but requires them to be implemented in a manner appropriate to distributed ledger technologies.

Privacy/ CLAUSE IN FOCUS

CONFIDENTIALITY AND PERSONNEL ACCESS CONTROLS

Access to personal data should be limited to personnel who require it for the performance of their authorized duties. Agreements should require processors to ensure that employees, contractors and authorized personnel are subject to appropriate confidentiality obligations and access personal data only on a need-to-know basis.

These clauses should also require processors to implement access controls and promptly revoke access where personnel no longer require it or cease to be involved in the services.

Draft Illustrative Clause

"The Processor shall ensure that access to Personal Data is limited to those personnel who require such access for the performance of the Services."

"The Processor shall ensure that all personnel authorized to process Personal Data are bound by confidentiality obligations, whether arising under contract or applicable law, and shall ensure that such obligations continue following the termination of their engagement where applicable"

Negotiation Points

Controller

- Require the processor to ensure that all authorized personnel are subject to legally enforceable confidentiality obligations.
- Confirm that confidentiality obligations continue after personnel leave the processor's organization where appropriate.
- Require the processor to promptly revoke access where personnel no longer require it for the services.

Processor

- Define authorized personnel broadly enough to include employees, contractors and temporary staff engaged in providing the services.
- Ensure confidentiality obligations may arise under employment contracts, contractor agreements or applicable law, rather than prescribing a single mechanism.
- Request a reasonable period to revoke access for personnel who cease to require access or leave the processor's organization, taking into account operational and security requirements

Clearly drafted confidentiality and personnel access provisions play an important role in ensuring that access to personal data remains appropriately restricted, accountability is maintained, and the risk of unauthorized disclosure is minimized throughout the processing lifecycle.

BYTE/WISE

Privacy/ COMPLIANCE SNAPSHOT

Purpose Mapping

Purpose mapping forms the foundation of privacy governance. It provides a structured method for identifying and documenting the business purpose behind each processing activity. Maintaining a documented record of the specified purpose for each processing activity and the applicable ground for processing enables organizations to demonstrate accountability, support regulatory compliance and identify processing activities that no longer align with their documented purpose.

Purpose Mapping Exercise

- Map each category of personal data to a clearly defined business purpose.
- Identify whether the processing is based on consent or another legitimate use under the DPDP Act, or another recognized processing ground under applicable law.
- Distinguish primary processing activities from secondary uses such as analytics, AI, profiling, marketing or product improvement.
- Ensure that privacy notices, internal data inventories, contractual documentation and operational practices consistently reflect the documented purpose.

Organizations should revisit purpose mapping whenever new products, technologies, AI capabilities, business processes or third-party service providers are introduced. Particular attention should be given to secondary processing activities that may develop over time, as these often create the greatest disconnect between documented purposes and actual operational practices.

Quick Self-Check for Organisations

- Can every category of personal data processed by the organization be linked to a clearly documented business purpose?
- Has an appropriate processing ground been identified for each processing activity?
- Do privacy notices, contractual documentation and internal records accurately reflect how personal data is processed?
- Are there processing activities that continue simply because they have always existed, rather than mapped to a defined business purpose?

By periodically reviewing why personal data is collected, how it is used and the basis on which it is processed, organizations can identify compliance gaps early, improve accountability and ensure that their documented governance framework continues to reflect operational reality.

Privacy

KNOWLEDGE
CORNER

Controller vs Joint Controller

BYTE/WISE

Controller vs Joint Controller

Every processing activity begins with identifying who decides why and how personal data will be processed. Where a single organization independently determines the purpose of processing and the essential means by which it will be carried out, it acts as the controller (or Data Fiduciary under the DPDP Act). The position becomes more complex where two or more organizations are involved in making those decisions. In many commercial arrangements, organizations collaborate to deliver a shared product, operate a common platform, undertake joint marketing campaigns, conduct research or provide integrated digital services.

Where each organization independently determines the purposes and essential means for its own separate processing activities, each remains an independent controller. However, where two or more organizations jointly participate in determining the purposes and essential means of processing, a joint controller relationship may arise. The assessment depends on the substance of the parties' involvement and their actual influence over the purposes and essential means of processing, rather than the contractual labels adopted by the parties.

The GDPR expressly recognizes this concept in Article 26, which provides that where two or more controllers jointly determine the purposes and means of processing, they are joint controllers. The Regulation requires them to determine, through a transparent arrangement, their respective responsibilities for complying with the GDPR, particularly in relation to transparency obligations and the exercise of data subject rights. This allocation of responsibilities is primarily an internal governance mechanism and does not prevent data subjects from exercising their rights against each joint controller in accordance with the GDPR.

The DPDP Act, 2023 does not establish an equivalent statutory framework specifically governing joint controllers. However, the definition of a Data Fiduciary contemplates that the purpose and means of processing may be determined "alone or in conjunction with other persons." Although the Act does not prescribe obligations comparable to Article 26 GDPR, this language recognizes that decisions regarding the purpose and means of processing may be made collaboratively.

In practice, organizations commonly address these arrangements through detailed contractual provisions that allocate operational responsibilities, including transparency obligations, responses to data principal or data subject requests, incident management, regulatory cooperation, retention, security responsibilities and liability allocation. These arrangements also address governance mechanisms such as decision-making processes and allocation of accountability for regulatory notifications, audit and cooperation obligations, and procedures for managing changes to the processing relationship.

Organizations should assess how decisions relating to the purpose of processing, the essential means of processing, transparency, data subject rights, security, retention and regulatory compliance are allocated in practice, and ensure that their governance and contractual arrangements accurately reflect those responsibilities.

BYTE/WISE

PART THREE

DIGITAL ASSETS

JULY 2026

Digital Assets / REGULATORY UPDATES

EU Plans to Review MiCA Rules to Include Non-EU Stablecoin Issuers

The Markets in Crypto-Assets Regulation (MiCA) is the European Union's (EU) first comprehensive framework for regulating crypto-assets and crypto service providers. It aims to establish a uniform regulatory regime across EU member states while strengthening investor protection and market stability. Since MiCA came into force earlier this year, it has significantly reshaped the EU's crypto landscape, with several crypto service providers restricting or discontinuing operations due to the new compliance requirements.

The European Commission is now reportedly considering amendments to MiCA to address regulatory gaps, particularly concerning stablecoins (digital assets designed to maintain a stable value by being linked to assets such as fiat currencies) and tokenization (the representation of ownership of real-world assets on a blockchain).

A key proposal is to bring certain non-EU stablecoin issuers and tokenized asset providers within the scope of MiCA where their products are offered or used in the EU. This would strengthen regulatory oversight of digital assets that impact EU markets, regardless of where the issuer is located. The proposed changes could also encourage international crypto businesses to re-enter the European market by providing greater regulatory certainty. This may improve market participation, enhance liquidity, and support wider institutional adoption of digital assets.

Although the amendments are still under consideration, they demonstrate the EU's continued commitment to balancing innovation with effective regulatory oversight and reinforcing its role in the evolving global digital asset ecosystem.

ASIC Extends Licensing Relief for Digital Asset Businesses in Australia

The Australian Securities and Investments Commission (ASIC) has extended its temporary no-action position for digital asset businesses until 30 September 2026, giving firms an additional three months to comply with Australia's financial licensing requirements. Under the no-action position, ASIC will not take enforcement action against eligible businesses transitioning to the new licensing framework, provided they satisfy the regulator's conditions.

The extension applies to businesses that need to obtain or vary an Australian Financial Services (AFS) license, as well as those requiring an Australian Market License or a Clearing and Settlement (CS) facility license. ASIC has also expanded the relief to cover businesses operating under authorized representative or intermediary arrangements with existing AFS license holders.

The relief supports the Australian Government's broader Digital Asset Framework reforms, which aim to provide greater regulatory certainty, encourage responsible innovation, and strengthen investor protection while ensuring a smooth transition to the evolving regulatory regime.

BYTE/WISE

RBI Reaffirms Its Stand on Cryptocurrency: No Legal Status Yet

On 2 July 2026, the Standing Committee on Finance met to discuss Virtual Digital Assets (VDAs), a term under Indian law that includes cryptocurrencies and certain digital tokens. During the meeting, the Reserve Bank of India (RBI) confirmed that it has not recommended granting legal status to cryptocurrencies.

Appearing before the Committee for the first time on this issue, the RBI reiterated its long-standing concerns that private cryptocurrencies could pose risks to financial stability, investor protection, anti-money laundering efforts, and the country's monetary system. The RBI has maintained a cautious stance on cryptocurrencies since 2013.

The Committee also reviewed the progress of the RBI's Central Bank Digital Currency (CBDC), the Digital Rupee (e₹). Although the Digital Rupee has recorded over 150 million transactions since its launch, its adoption remains modest compared to the Unified Payments Interface (UPI).

In addition, the Institute of Chartered Accountants of India (ICAI) highlighted practical challenges in auditing VDAs under the existing tax regime and suggested that greater regulatory clarity may be needed.

Despite India having an estimated 119 million cryptocurrency users, there is still no dedicated law governing cryptocurrencies. The sector continues to be regulated primarily through taxation, including a 30% tax on VDA gains, 1% Tax Deducted at Source (TDS) on transactions, and applicable Goods and Services Tax (GST) on trading fees.

The Committee's discussions did not lead to any regulatory or policy changes. The current tax framework remains in place, and the RBI continues to oppose legal recognition of private cryptocurrencies. The Committee is expected to study global regulatory approaches before making its recommendations. Until then, India's regulatory position on cryptocurrencies remains unchanged.

BYTE/WISE

Hong Kong Completes Its Crypto Regulatory Framework

Hong Kong has taken another major step towards becoming a leading hub for the virtual asset ("VA") industry. On 26 May 2026, the Financial Services and Treasury Bureau ("FSTB") and the Securities and Futures Commission ("SFC") released the consultation conclusions for introducing licensing regimes for VA advisory and VA management services. These reforms build on the proposed licensing frameworks for VA dealing and VA custody announced in 2025, creating a more comprehensive regulatory system for crypto-related businesses.

Under the new framework, VA advisory refers to providing recommendations, research, trading signals, or reports that help investors decide whether, when, or how to buy or sell virtual assets. This may also include algorithm-based recommendations and copy-trading services. However, products such as tokenized securities and crypto derivatives that are already regulated under Hong Kong's securities laws will continue to remain outside the scope of the new VA advisory license.

The proposed VA management regime will apply to businesses managing portfolios of virtual assets on behalf of clients. Unlike the existing securities regime, there will be no minimum threshold for crypto exposure before a license is required. Fund managers investing in virtual assets alongside traditional securities may therefore need licenses under both regulatory regimes.

The regulators have also clarified that certain exemptions will apply. For example, businesses providing advisory or management services only to wholly owned group companies may not require a separate license. Similarly, licensed VA managers carrying out trading solely for portfolio management purposes will not need an additional dealing license.

To obtain a license, firms must establish a local presence in Hong Kong, appoint qualified and experienced personnel, maintain effective risk management systems, and comply with investor protection requirements. Capital requirements will depend on whether the business holds client assets, with higher financial thresholds applying to firms undertaking custody functions.

The Hong Kong Government is expected to introduce legislation later this year to formally implement the licensing framework for VA dealing, custody, advisory, and management services. Existing market participants are encouraged to begin engaging with the SFC early, as no automatic transition period will be available once the new regime comes into force.
With these reforms, Hong Kong is aligning itself with jurisdictions such as the European Union, Singapore, and the United Arab Emirates by adopting a comprehensive regulatory framework for virtual assets. The new regime aims to strengthen investor protection, enhance market integrity, and support the sustainable growth of Hong Kong's digital asset ecosystem.

Digital Assets / CLAUSE IN FOCUS

TOKEN DELISTING CLAUSE

As the digital asset ecosystem continues to develop, cryptocurrency exchanges regularly review the tokens available on their platforms. A token may be delisted for several reasons, including changes in law, security vulnerabilities, low trading volumes, network failures, or where the project no longer meets the platform's listing standards. While exchanges require the flexibility to remove risky or non-compliant tokens, users often expect sufficient notice and a fair opportunity to withdraw or transfer their holdings before support is discontinued.

A token delisting clause seeks to balance these competing interests. It enables the platform to respond promptly to regulatory or operational risks while providing users with greater transparency regarding the circumstances under which a token may be delisted and the process that will follow.

Draft Illustrative Clause

"The Platform may, at its reasonable discretion, suspend trading, discontinue support for, or delist any Digital Asset where it determines that such action is necessary due to applicable law or regulatory requirements, security concerns, technological vulnerabilities, insufficient market liquidity, network instability, or where the Digital Asset no longer satisfies the Platform's listing standards. Where reasonably practicable, the Platform shall provide prior notice of the proposed delisting and specify the period during which Users may continue to trade or withdraw the affected Digital Asset. Upon expiry of such period, the Platform may suspend deposits, trading, and withdrawals relating to the affected Digital Asset. The Platform shall not be liable for any loss arising from fluctuations in the value of the Digital Asset or the delisting decision, except where such loss results from the Platform's gross negligence, wilful misconduct, or fraud."

Negotiation Points

Exchange

- Retain the right to delist a Digital Asset where required due to regulatory, security, technical, liquidity, or commercial considerations.
- Preserve the ability to take immediate action where continued listing may expose the Platform or its users to legal or operational risks.
- Limit liability for losses resulting from market movements or the delisting of a Digital Asset, except where expressly assumed.
- Reserve the right to suspend deposits, trading, and withdrawals independently where necessary to protect the Platform or comply with applicable law.

User / Institutional Customer

- Seek clearly defined grounds on which a Digital Asset may be delisted, rather than granting the Platform unrestricted discretion.
- Seek protection against the Platform automatically selling, converting, or otherwise disposing of Digital Assets without the user's prior consent, unless required by applicable law.
- Ensure an adequate withdrawal period so that users have sufficient time to transfer their Digital Assets to another wallet or platform.
- Request transparency regarding the reasons for the delisting and any available alternatives for affected users.

A well-drafted token delisting clause recognizes that while exchanges must have the flexibility to respond quickly to changing regulatory and market conditions, users should not be left without adequate notice or access to their assets.

Digital Assets

KNOWLEDGE
CORNER

Decentralized Finance (DeFi): The Next Frontier in Digital Assets

BYTE/WISE

Decentralized Finance ("DeFi") has emerged as one of the most significant innovations in the digital assets ecosystem. It refers to a blockchain-based financial system that enables users to access services such as trading, lending, borrowing, and payments without relying on traditional intermediaries like banks or financial institutions. Instead, transactions are executed through smart contracts, self-executing programs deployed on blockchain networks.

Most DeFi applications are built on public blockchains such as Ethereum, although networks like Solana, Avalanche, and BNB Chain also support thriving DeFi ecosystems. Users typically interact with these protocols through non-custodial digital wallets, allowing them to retain control of their assets while participating in decentralized financial activities.

One of the core pillars of DeFi is the Decentralized Exchange ("DEX"), which allows users to trade digital assets directly from their wallets. Unlike traditional exchanges, many DEXs rely on Automated Market Makers ("AMMs"), where users provide liquidity to shared pools and earn a portion of the transaction fees.

DeFi also enables lending and borrowing without conventional credit assessments. Users may lend their digital assets to earn interest or borrow assets by providing collateral, with smart contracts automatically managing repayments and liquidations. In addition, stablecoins, which are digital assets designed to maintain a relatively stable value, play a crucial role in facilitating payments, trading, and lending while reducing the impact of price volatility.

The rapid growth of DeFi has been driven by several advantages. By eliminating intermediaries, DeFi can reduce transaction costs and enable faster settlement of transactions. Public blockchains also provide greater transparency, allowing users to independently verify transactions and protocol operations. Further, DeFi promotes financial inclusion by making financial services accessible to anyone with an internet connection and a compatible digital wallet.

Despite these benefits, DeFi presents significant risks. Smart contract vulnerabilities remain one of the sector's biggest challenges, with coding flaws potentially exposing users to substantial financial losses. Digital asset price volatility may trigger automatic liquidations of collateral, while governance of many DeFi protocols through Decentralized Autonomous Organizations ("DAOs") raises questions around accountability and decision-making. The pseudonymous nature of blockchain transactions also presents challenges relating to anti-money laundering ("AML"), consumer protection, and sanctions compliance.

Regulators across the globe are increasingly evaluating how existing financial laws apply to DeFi. While the European Union's Markets in Crypto-Assets Regulation ("MiCA") primarily regulates crypto-asset service providers, the treatment of fully decentralized protocols continues to evolve. Similarly, regulators in jurisdictions such as the United States, Singapore, and the United Arab Emirates are actively assessing DeFi activities within their broader digital asset regulatory frameworks. In India, there is currently no dedicated legal framework governing DeFi, although existing laws relating to taxation, AML, foreign exchange, and securities may apply depending on the nature of the activity.

As blockchain adoption continues to expand, DeFi is expected to play an increasingly important role in the future of financial services. However, its long-term success will depend on balancing innovation with robust governance, cybersecurity, and regulatory certainty to foster a secure and sustainable digital financial ecosystem.

BYTE/WISE

PART FOUR

DARK PATTERNS

JULY 2026

BASKET SNEAKING

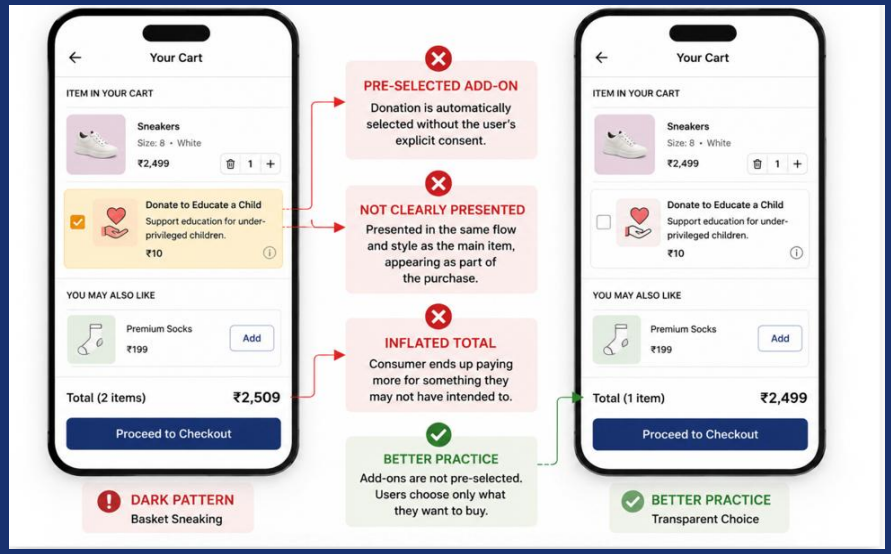
Definition:

Basket Sneaking occurs when a seller automatically adds additional products, services or charges to a consumer's shopping cart or payment journey without the consumer's explicit and informed consent, requiring the consumer to actively remove them before completing the transaction.

Following the CCPA's recent enforcement action against PhysicsWallah, where the Authority found that a pre-selected ₹10 donation had been automatically added during checkout without explicit consumer consent, Basket Sneaking has emerged as one of the first dark patterns to be the subject of direct regulatory enforcement in India. The Authority reiterated that consumer consent cannot be presumed through pre-selected options and must instead be obtained through a clear affirmative action.

Examples:

- ❌ Automatically adding donations, extended warranties, insurance, memberships or other paid add-ons to a shopping cart through pre-selected options.
- ❌ Including optional products or services by default and requiring consumers to remove them before completing their purchase.
- ❌ Bundling optional charges into the final payable amount in a manner that may reasonably lead consumers to believe they form part of the primary purchase.



Better practice

- ✅ Ensure all optional products, services and charges are added only after an explicit affirmative action by the consumer.
- ✅ Clearly distinguish optional add-ons from mandatory charges and present them separately during checkout.
- ✅ Provide consumers with a clear order summary before payment, enabling them to easily identify and review every item and charge included in the transaction.

Tip for businesses

Regularly audit checkout and payment journeys to identify any pre-selected or automatically added products, services or charges. Optional additions should require an active consumer choice, supported by transparent pricing and neutral interface design that enables consumers to make free and informed purchasing decisions.

COMING SOON

AUGUST 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