BYTE/WISE

emerging tech decoded

LEX CONSULT EDITORIAL

BYTE/WISE

KEY HIGHLIGHTS

DEC 2025

Artificial Intelligence

Regulatory Updates

- Proposed amendments to the EU AI Act
- EDPS issues guidance on AI Risk Management
- Singapore consults on AI Risk Management Guidelines
- United States Moves Toward a Federal AI Policy Framework
- India Considers Statutory Royalties for Copyrighted Works Used in AI Training

Clause in Focus - AI Output Liability and Safe-Use

Compliance Snapshot - Responding to Harmful AI Outputs

Knowledge Corner - General-Purpose AI Model vs. High-Risk AI System

Privacy

Regulatory Updates

- EU Digital Omnibus Package
- Additional provisions now in effect for UK’s Data (Use and Access) Act
- EU EDPB Issues Draft Guidance on Mandatory User Accounts under the GDPR
- California: Privacy Enforcement Moves from Rulemaking to Execution

Clause in Focus - Personal Data Breach

Compliance Snapshot - Notice and Consent Requirements under the DPDP Rules

Knowledge Corner - Anonymized Data vs Pseudonymized Data

Digital Assets

Regulatory Updates

- The Property (Digital Assets etc) Act: A Landmark in UK Property Law
- ESMA Issues MiCA Data Standards
- Canada Signals Stricter Regulatory Treatment of Stablecoins
- Japan Tightens Supervisory Expectations for Crypto Asset Custody and Exchanges
- US Regulators Begin Implementing the GENIUS Act Stablecoin Framework

Clause in Focus - Force Majeure and Cyber Risk in Crypto Custody Agreements

Knowledge Corner - Navigating India's Crypto Landscape:
Centralized vs. Decentralized Exchanges

Dark Patterns Check – Forced Action

PART ONE

Ai

Ai / REGULATORY UPDATES

Proposed amendments to the EU AI Act

On 19 November 2025, the European Commission released a ‘*Digital Package*’, proposing targeted amendments to the EU AI Act. The proposals seek to ease compliance burdens and improve regulatory clarity, while preserving the statute’s core risk-based safeguards.

Key Highlights of the amendment are as follows:

- Deferred application of high-risk AI obligations: Application of high-risk requirements would be deferred, with Annex III systems subject to a backstop date of 2 December 2027, and Annex I systems (linked to EU harmonized product legislation) subject to a backstop date of 2 August 2028.

- Reduced registration requirements for exempt systems: Certain AI systems treated as not high-risk under the Act’s exemption framework would no longer require registration in the EU database.

- Streamlined conformity assessment: The proposal clarifies how conformity assessments apply where AI systems fall under EU harmonized product legislation, with the aim of avoiding duplicative assessments and enabling more integrated, single-assessment compliance pathways.

- Bias-mitigation processing under data protection law: The amendments expressly enable limited processing of special category personal data for bias detection and correction, subject to strict safeguards and continued compliance with GDPR requirements.

- Refined enforcement role for the AI Office: The AI Office (an office set out under the EU AI Act to oversee the implementation) would assume exclusive market surveillance competence in defined cases, including certain AI systems based on general-purpose AI models and systems embedded in very large online platforms and search engines.

In addition, the proposal includes institutional and implementation-oriented clarifications, including enhanced coordination between national regulatory sandboxes, a clearer basis for limited EU-level involvement via the AI Office in supervised real-world testing, and a shift in responsibility for promoting AI literacy from individual providers and deployers to the Commission and Member States.

Organizations should continue preparing for high-risk compliance while monitoring how deferrals, conformity-assessment pathways, sandbox participation, and AI Office supervision may affect implementation planning and cross-border AI deployments as the Digital Omnibus package proceeds through the EU legislative process.

EDPS issues guidance on AI Risk Management

On 11 November 2025, the European Data Protection Supervisor (EDPS) issued guidance on AI risk management for EU institutions acting as controllers under Regulation (EU) 2018/1725, having relevance for private organizations processing personal data through AI systems. The guidance emphasizes a structured, lifecycle-based approach to AI risk management, with key expectations including:

- Lifecycle-wide risk management: Controllers are expected to identify and mitigate data protection risks at each stage of the AI lifecycle, including data collection, model training, deployment, monitoring, and retirement.

- ISO 31000 alignment: Risk assessments should follow a structured methodology, with documented risk identification, impact and likelihood scoring, mitigation measures, and periodic review.

- Four priority risk areas:

  - *Fairness*: Ongoing testing and monitoring for bias and discriminatory outcomes.

  - *Accuracy*: Controls to identify, correct, and prevent erroneous or misleading outputs.

  - *Data minimization*: Limits on training and inference data, including justification for feature selection.

  - *Security*: Safeguards against data leakage, model inversion, and adversarial attacks.

- Interpretability and explainability: AI systems should be designed to enable meaningful understanding of how outputs are generated, enabling human oversight and effective challenge of automated decisions.

The EDPS guidance signals rising regulatory expectations around documented governance, technical controls, and continuous monitoring of AI systems. Organizations deploying AI that processes personal data should treat AI risk management as an ongoing compliance function, integrated with DPIAs, security controls, and accountability frameworks.

Singapore consults on AI Risk Management Guidelines

On 13 November 2025, the Monetary Authority of Singapore (MAS) published a consultation paper proposing comprehensive '*Guidelines on AI Risk Management*' for financial institutions. The consultation is open until 31 January 2026. The proposed guidelines set out supervisory expectations on governance structures, lifecycle risk controls, oversight practices, and capability frameworks for AI risk management in the financial sector.

Key elements include:

- Expectations for board and senior management oversight of AI risk frameworks.

- Clear identification and inventory of AI use cases within firms.

- Lifecycle controls covering data management, fairness, explainability, human oversight, third-party risk, monitoring, and change management.

- Proportionate application of controls based on risk profile and AI usage.

The draft guidelines expressly cover a broad range of AI technologies, including generative and agent-based AI systems, and MAS has indicated that an implementation period of approximately 12 months is expected following finalization. While MAS has previously issued principles-based guidance on ethical AI use, such as the FEAT Principles and the Model AI Governance Framework, the proposed guidelines mark a shift toward more formalized, supervisory expectations for AI risk management within regulated financial institutions.

United States Moves Toward a Federal AI Policy Framework

On 11 December 2025, U.S. President Donald Trump signed an executive order aimed at establishing a national policy framework for artificial intelligence, signaling a shift toward stronger federal coordination of AI governance. The order directs federal agencies to review existing state-level AI laws and assess whether they conflict with federal objectives, particularly in areas such as bias regulation, transparency obligations, and compliance burdens.

The executive order also initiates the creation of a federal AI Litigation Task Force and frames AI regulation as a matter of national competitiveness, explicitly cautioning against a fragmented state-by-state approach. While the order does not itself pre-empt state laws, it is expected to trigger legal and political challenges that could shape the balance between federal authority and state-level AI regulation in the United States over the coming year.

India Considers Statutory Royalties for Copyrighted Works Used in AI Training

An expert committee constituted under India's Department for Promotion of Industry and Internal Trade (DPIIT) has released a working paper proposing a statutory framework that would require AI developers to pay royalties for the use of copyrighted works in AI training. The proposal is intended to address compensation concerns arising from large-scale use of copyrighted content in generative AI development.

Key elements of the proposal include:

- A compulsory licensing model for copyrighted works used in AI training, replacing voluntary or bilateral licensing.
- A proposed "one nation, one license, one payment" structure, with statutory remuneration paid to a central collecting mechanism.
- No opt-out for rights holders, with compensation framed as a statutory entitlement rather than consent-based access.
- Policy support from the Ministry of Electronics and Information Technology (MeitY), which has publicly favored a mandatory licensing approach.

In the global context, the proposal reflects a highly interventionist approach to AI training data governance. Conceptually, it resembles statutory copyright remuneration systems administered by collecting societies but applies this model to upstream AI training rather than downstream public use. If taken forward, the proposal would position India as a jurisdiction asserting strong public-interest control over AI training economics, diverging from both the EU's text-and-data-mining exceptions and the more litigation-driven U.S. approach to AI copyright disputes.

Ai / CLAUSE IN FOCUS

AI OUTPUT LIABILITY AND SAFE-USE

AI models generate probabilistic outputs rather than guaranteed facts. As noted in our October edition, recent legislative and enforcement signals in jurisdictions such as California and parts of Europe reflect a growing regulatory emphasis on human accountability for unsafe AI deployment. Across emerging AI governance frameworks, responsibility for AI-related harm is increasingly being placed on the organizations that design, deploy, or rely on AI systems, rather than on the technology itself.

To manage output-related risk, contracts are increasingly introducing clauses that:

- Limit blind reliance on AI outputs;
- Define permitted and prohibited use cases;
- Allocate responsibility based on control, modification, and deployment
- provide indemnities where systems are misused or deployed outside agreed parameters.

Draft Illustrative Clause

"Safe-Use Indemnity: The Deployer agrees to indemnify and hold harmless the Provider against any claims, liabilities, fines, or damages arising from: (i) reliance on AI-generated outputs without required human review, (ii) modification or fine-tuning of the model without Provider's approval, (iii) integration with unapproved datasets or systems, or (iv) deployment of the AI system in prohibited or high-risk scenarios not disclosed to the Provider. This indemnity shall not apply to harm caused by the Provider's wilful misconduct or known defects or limitations that were not disclosed to the Deployer"

Negotiation Points

Deployer

- Carve out indemnity where harm arises from known defects, biased training data, or undocumented limitations, or misleading performance representations by the Provider.
- Clearly define permitted, prohibited, and high-risk use cases in an exhaustive schedule, limited to pre-agreed deployment scenarios.
- Provide appropriate representations and warranties along with full disclosures with respect to known system limitations, intended use restrictions, and material risk characteristics of the AI system.

Provider

- Ensure the indemnity clearly captures unreviewed reliance, unauthorized fine-tuning, shadow integrations, and undisclosed downstream deployments.
- Require the Deployer to disclose intended high-risk uses upfront, with failure to do so constituting waiver from the indemnity protection.
- Limit liability for downstream decisions outside documented specifications and keep liability caps tied to fees paid, excluding indirect or consequential losses.
- Require express acknowledgment that AI outputs are non-deterministic, require human validation and are not professional or factual guarantees.

Providers typically seek to limit liability for downstream decisions and misuse of AI systems, while deployers aim to confine indemnities to clear deviations from agreed use cases. Balanced drafting should align contractual risk allocation with real control over deployment and reliance on outputs, ensuring accountability without constraining legitimate AI use.

Ai / COMPLIANCE SNAPSHOT

Responding to Harmful AI Outputs

As AI systems are increasingly used to generate content and support decisions, organizations must be prepared for incidents where the output itself causes harm, such as, inaccurate information, biased recommendations, unsafe advice, or misleading synthetic content. Under various upcoming legislations, including the EU AI Act, such failures fall within the risk management, post-market monitoring, and human oversight obligations framework. Monitoring how outputs are identified, escalated, and corrected allows providers and deployers to demonstrate that risk controls remain effective in practice, rather than existing only at the design or documentation stage

What an AI Output Incident Response should cover:

- *Corrective and preventive actions*: Implementation and documentation of corrective measures, including model updates, data adjustments, or deployment constraints, to address identified output-related risks.

- *Human oversight intervention*: Mechanisms enabling designated human oversight functions to suspend, restrict, or adjust system use where outputs indicate risks not adequately mitigated at design or deployment stage.

- *Post-market monitoring triggers*: Procedures to detect output anomalies or failures as part of the post-market monitoring system required under the AI Act, including signals indicating residual or emerging risks

- *Incident documentation and traceability*: Maintenance of records demonstrating how output incidents were identified, assessed, and addressed, in line with quality management and record-keeping obligations.

Key Compliance Questions

- How are high-risk or low-confidence outputs identified and escalated?

- Do human oversight arrangements allow timely intervention, suspension, or restriction of system use when outputs indicate risk?

- Who has authority to halt or override AI-driven decisions?

- When does an AI output issue trigger user notification or regulator engagement?

- Are incident logs sufficient to demonstrate effective monitoring, corrective action, and ongoing compliance?

Harmful or incorrect AI outputs should be treated as compliance-relevant events rather than isolated system errors. Deployers should not treat model behavior or vendor reliance as a transfer of regulatory responsibility, embedding post-market monitoring, human-oversight intervention, and documented corrective-action mechanisms into deployment workflows and contractual arrangements is central to meeting obligations under the EU AI Act and managing supervisory risk.

Ai

KNOWLEDGE
CORNER

General-Purpose AI Model vs. High-Risk AI System

Defined Terms (EU AI Act)

General-Purpose AI Model (GPAI Model)

Under the EU AI Act, a General-Purpose AI model refers to an AI model, including large generative models, that is trained on broad datasets and is capable of performing a wide range of tasks, and that can be adapted or integrated into multiple downstream applications across different sectors and use cases.

High-Risk AI System

A High-Risk AI System is an AI system that is either:

(a) used as a safety component of a product, or is itself a product, covered by EU harmonization legislation (such as medical devices, machinery, or vehicles); or

(b) deployed in specifically listed sensitive use-cases set out in Annex III of the EU AI Act, including areas such as biometric identification, employment, creditworthiness, access to education, law enforcement, migration, and essential public services.

Explanation

The EU AI Act draws a critical distinction between model capability and deployment risk. General-Purpose AI models are regulated based on their breadth and adaptability, whereas High-Risk AI systems are regulated based on their context of use and impact on fundamental rights and safety. A GPAI model is not inherently high-risk. It becomes subject to heightened regulatory scrutiny only when it is integrated into, or used to build, a high-risk AI system. The risk classification therefore attaches primarily at the system and use-case level, not merely at the model level.

For example, a large language model capable of text generation, translation, and summarization would qualify as a GPAI model. If that same model is deployed within a recruitment tool used to screen job applicants, or within a credit-scoring or loan-eligibility system that influences access to financial services, the resulting application may qualify as a High-Risk AI System under Annex III, triggering a significantly higher compliance burden.

This distinction has significant implications for liability allocation, contracting, and compliance design. A single GPAI model may be embedded into dozens of downstream applications, only some of which qualify as high-risk. For organizations building or integrating AI solutions, this means that compliance cannot be assessed in isolation. A low-risk GPAI model may still create high-risk regulatory exposure once deployed in sensitive operational contexts. Clear contractual role-mapping between model providers, system integrators, and deployers is essential to ensure that risk-management, documentation, and oversight obligations are properly allocated.

PART TWO

PRIVACY

Privacy / REGULATORY UPDATES

EU Digital Omnibus Package

On 19 November 2025, the European Commission published proposed amendments to the GDPR under its Digital Omnibus package, aimed at clarifying key concepts and improving consistency of application across Member States. Key proposed changes include:

- *Scope of "Personal Data"*: Sets out that the scope of what qualifies as personal data may differ depending on the controller's access to the *means reasonably likely to be used* to identify an individual. In practice, the same dataset may be treated differently across entities based on access to re-identification keys, auxiliary information, technical capabilities, and legal or organizational constraints.

- *Treatment of Pseudonymized data*: Introduces circumstances in which pseudonymized data may not qualify as personal data for certain entities where identification of the data subject is not reasonably likely using the means available to them.

- *AI-related processing*: Addresses the circumstances in which legitimate interest may be relied upon for certain AI development and operational activities, such as system testing, performance monitoring, or bias mitigation and clarifies how the processing of special category data in AI contexts remains subject to necessity, proportionality, and existing GDPR safeguards.

- *Operational amendments*: Proposes targeted adjustments to GDPR compliance mechanisms, including extending flexibility around personal data breach notification timelines beyond the current 72-hour framework, and further harmonization of data protection impact assessment and data subject access request procedures across Member States.

The proposed shift toward an entity-specific assessment of personal data scope could materially affect how organizations classify and manage data, particularly in analytics and AI development contexts where access to re-identification keys or auxiliary data is limited. While this may reduce GDPR obligations for certain actors, it also heightens the need for robust documentation of identifiability assumptions, access controls, and re-identification risk. Critics also argue that some proposed amendments may constrain data subject rights in practice. As noted in an earlier Bytewise update on the Digital Omnibus initiative, these proposals build on a broader shift toward a contextual and risk-based assessment of identifiability under the GDPR, moving away from a uniform, abstract approach to personal data classification.

Additional provisions now in effect for UK's Data (Use and Access) Act

Provisions of the Data (Use and Access) Act 2025 (DUAA) relating to law enforcement data processing and digital verification services have now entered into force, marking the near completion of Stage Two of the DUAA's four-phase implementation timeline. The DUAA is a wide-ranging reform that amends, but does not replace, the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations, with the aim of promoting responsible data use and innovation alongside core privacy protections.

With effect from 17 November 2025, sections 89 and 90 of the DUAA came into force, introducing new rules governing joint processing of personal data for law-enforcement and intelligence-service purposes. Shortly thereafter, the DUAA (Commencement No. 4) Regulations 2025 brought Part Two of the Act (digital verification services) into force from 1 December 2025, excluding provisions on information-sharing by public authorities with registered verification providers. Part Two establishes a statutory framework for digital verification services, covering registered public and private entities providing trusted identity or attribute verification (such as age, identity, or residency). While these provisions do not themselves amend individual data subject rights, they facilitate structured joint processing and controlled data sharing under regulatory oversight.

The UK Government has indicated that the bulk of the DUAA's substantive data-protection amendments, including changes affecting subject access requests and lawful processing grounds, are expected to enter into force in early 2026, with updated ICO guidance anticipated as implementation progresses.

EU EDPB Issues Draft Guidance on Mandatory User Accounts under the GDPR

On 4 December 2025, the European Data Protection Board (EDPB) adopted Recommendations 2/2025 on the legal basis for requiring users to create accounts on e-commerce websites. The Recommendations have been released for public consultation until 12 February 2026. The EDPB addresses a common but under-examined design choice: whether users can be compelled to create an account as a condition for accessing certain online services, particularly e-commerce services.

The recommendations clarify that:

- Mandatory account creation must be justified under a valid GDPR lawful basis (Article 6), assessed case by case.

- Controllers cannot rely on convenience or commercial preference alone to mandate account creation.

- In many standard e-commerce scenarios, requiring an account may be incompatible with data minimization if the service can reasonably be offered through a guest or account-optional model.

- Where controllers rely on contractual necessity, the account requirement must be objectively necessary to perform the contract, not merely useful.

- Reliance on legitimate interests requires a documented balancing test demonstrating that the account requirement does not override data subject rights and expectations.

The Recommendations explicitly link mandatory account design to the GDPR's privacy-by-design and default obligations under Article 25, signaling a shift from regulating how personal data is processed to scrutinizing whether certain data-collection architectures are justified at all. In doing so, the EDPB flags increasing regulatory attention on platform design choices that structurally expand personal data collection, "account-first" models that are not objectively required for service delivery, and blanket reliance on legitimate interests without a meaningful necessity and balancing analysis.

California: Privacy Enforcement Moves from Rulemaking to Execution

In November 2025, the California Privacy Protection Agency (CPPA) announced the creation of a Data Broker Enforcement Strike Force, signaling a move from rulemaking toward active supervisory enforcement under the California Consumer Privacy Act (CCPA) and the Delete Act. Under California privacy law, *a data broker* refers to an entity that knowingly collects and sells or shares personal information about consumers with whom it does not have a direct relationship, typically for independent commercial purposes.

The initiative focuses on identifying and pursuing non-compliance by data brokers that fail to register, honor deletion requests, or meet statutory transparency obligations. Although the Strike Force is framed around data brokers, the implications extend more broadly. Many platforms, ad-tech intermediaries, analytics providers, and data-driven service vendors fall within, or adjacent to, California's expansive conception of data brokerage and may therefore face increased regulatory scrutiny as California's privacy regime enters a more enforcement-focused phase heading into 2026.

Privacy/ CLAUSE IN FOCUS

PERSONAL DATA BREACH

Personal data breach clauses allocate responsibility for detection, escalation, notification, and remediation when personal data is compromised. Under the DPDP framework, statutory breach notification obligations rest primarily with the Data Fiduciary, but breaches often originate within processor-controlled environments. Contractual clarity is therefore essential to ensure timely information flow and coordinated response, while distinguishing routine security incidents from notifiable personal data breaches.

Draft Illustrative Clause

"In the event the Processor becomes aware of any Security Incident involving Personal Data that has resulted in, or is reasonably likely to result in, a Personal Data Breach, the Processor shall notify the Data Fiduciary without undue delay. Such notification shall include all information reasonably available to the Processor regarding the nature of the breach, the categories of Personal Data affected, the approximate number of Data Principals concerned, the likely consequences of the breach, and the measures taken or proposed to address and mitigate its effects. The Processor shall cooperate with the Data Fiduciary in investigating, containing, and remediating the Personal Data Breach."

Negotiation Points

Data Fiduciary

- Seek defined notification timelines (e.g. immediate notice or within a specified number of hours) from the point at which the Data Processor becomes aware of a qualifying incident, to ensure sufficient time for internal assessment and external notification obligations.

- Mandate cooperation obligations covering investigation, containment, evidence preservation, and root-cause analysis, rather than notification alone.

- Ensure the clause clearly assigns breach classification and notification authority to the fiduciary.

- Seek liability allocation that holds the Data Processor responsible for failures in timely notification, cooperation, or incident containment within the processor's control.

Data Processor

- Distinguish clearly between security incidents and personal data breaches, limiting notification obligations to incidents that adversely affect personal data.

- Resist rigid or absolute timelines in favour of "without undue delay". Limit reporting to information reasonably available at the time, with express allowance for staged or supplemental updates as investigations progress.

- Align cooperation and remediation obligations with technical feasibility and the processor's actual control over systems, logs, and infrastructure.

- Limit liability to direct losses arising from the processor's breach of contractual obligations (e.g. delayed notification or failure to cooperate), and exclude liability for regulatory penalties.

Data Fiduciaries typically seek rapid notification, auditability, and clear escalation pathways to preserve regulatory timelines and accountability, while Data Processors prefer flexibility to accommodate incident investigation, technical constraints, and staged fact-finding. Balanced drafting should align contractual breach obligations with real operational capabilities.

Privacy/ COMPLIANCE SNAPSHOT

Notice and Consent Requirements under the DPDP Rules

The Digital Personal Data Protection Rules, 2025 operationalize notice and consent requirements under the DPDP Act by prescribing how notice must be presented, how consent must be obtained, and how it must be withdrawn, primarily through Rules 3, 4, and 6. Compliance with these notice, consent, and withdrawal requirements rests with the Data Fiduciary, which bears primary responsibility for ensuring the lawfulness of personal data processing under the DPDP framework.

Rules 3 & 4 (Notice and Consent): A Data Fiduciary is required to issue a standalone, clear, and plain notice, independent of other information, specifying: (i) the personal data proposed to be processed; (ii) the specified purpose(s) of processing; (iii) the manner of consent withdrawal and the consequences of such withdrawal; and (iv) accessible grievance redressal details. Consent may be obtained only after such notice is provided, must be linked to the specified purpose, expressed through a clear affirmative action, must not be inferred from silence or inactivity, must not be bundled across unrelated purposes, and must not be made a condition for availing goods or services unless processing is necessary for that purpose.

Rule 6 (Withdrawal of Consent): Withdrawal of consent must be as easy as the method used to give consent, available through accessible means, and upon withdrawal, the Data Fiduciary must cease processing within a reasonable time, unless continued processing is otherwise permitted under the DPDP Act or any other applicable law.

The DPDP Rules treat notice, consent, and withdrawal as inseparable elements of lawful processing, rather than isolated formalities. Any defect in notice content, consent sequencing, or withdrawal design directly affects the legality of processing thereby calling into question the lawfulness of the entire data lifecycle, including subsequent use, sharing, and disclosure of personal data.

Quick Self-Check for Organizations

- Does the notice clearly and specifically identify the personal data proposed to be processed, the specified purpose(s), the consent withdrawal method, and the grievance redressal channel?

- Is consent captured only after notice is displayed and through an affirmative action?

- Is the consent withdrawal mechanism as simple and accessible as the method used to give consent?

- Are consent, withdrawal, and sequencing events logged and retrievable to demonstrate compliance if required?

Privacy

KNOWLEDGE
CORNER

Anonymized Data vs Pseudonymized Data

Anonymized Data vs Pseudonymized Data

Anonymization and pseudonymization are distinct data-processing techniques that carry different legal consequences under modern data protection frameworks, particularly for compliance scope, risk allocation, and permissible use.

Anonymized data refers to data that has been processed in such a way that an individual can no longer be identified, directly or indirectly, by any party using *reasonably likely means*. Recital 26 of the GDPR clarifies that, in assessing whether data relates to an identifiable individual, account must be taken of all means reasonably likely to be used for identification, including the cost, time, and technological effort involved; where identification would require disproportionate effort, the data may be considered anonymous and therefore fall outside the scope of the GDPR. For example, aggregate statistics showing average transaction values across a city, with no identifiers or linkage keys retained, would typically be considered anonymized.

Pseudonymized data refers to personal data that has been processed to limit direct identifiability, while preserving the possibility of re-identification. This concept is crystallized in Article 4(5) of the GDPR, which defines pseudonymization as processing that replaces identifying elements with artificial identifiers where re-linking remains possible through additional information kept separately. Because re-identification remains feasible, pseudonymized data continues to qualify as personal data and remains subject to all core GDPR principles, including purpose limitation, security safeguards, and accountability. For example, replacing customer names with unique user IDs while storing the mapping separately constitutes pseudonymization, not anonymization. The GDPR treats pseudonymization as a risk-mitigation measure, explicitly recognizing it as an appropriate technical and organizational safeguard.

Anonymization, on the other hand, operates as a scope-determining endpoint in the data lifecycle and a form of regulatory risk mitigation, at which point the data ceases to qualify as personal data and falls outside the scope of most data protection laws.

The Digital Personal Data Protection Act, 2023 does not expressly define anonymization or pseudonymization, but applies only to *digital personal data*, defined as data about an identifiable individual. On this basis, personal data that has been irreversibly anonymized should fall outside the scope of the DPDP framework. Where identifiability is preserved, the data would continue to qualify as personal data under the Act.

PART THREE

DIGITAL ASSETS

The Property (Digital Assets etc) Act: A Landmark in UK Property Law

On December 2, 2025, the United Kingdom enacted the Property (Digital Assets etc) Act, a pivotal piece of legislation that formally recognizes cryptocurrencies and stablecoins as legal property. This Act, which received royal assent, marks a significant modernization of English property law by establishing a distinct third category for digital assets, thereby resolving previous legal ambiguities.

Historically, English property law categorized assets into "things in possession" (tangible objects) and "things in action" (enforceable rights, such as debts). Digital assets, being intangible and not readily fitting these traditional classifications, previously occupied an uncertain legal status, often addressed through fragmented common law judgments. The new Act addresses this gap by providing a statutory framework that expressly recognizes personal property rights in digital assets, including cryptocurrencies and non-fungible tokens (NFTs).

This legislation delivers several important legal and practical outcomes:

- Confirms that digital assets can be owned, inherited, and recovered in cases of theft.
- Allows inclusion of digital assets in insolvency and estate proceedings.
- Provides legal certainty and protections for individuals and businesses, fostering investor confidence.
- Reduces litigation by removing the need for courts to determine the property status of digital assets.
- Strengthens the attractiveness of English, Welsh, and Northern Irish law for crypto-related matters.

It is worth noting that the Act adopts a deliberately principle-based formulation. Rather than exhaustively defining which digital assets qualify as property, it clarifies that a thing is not excluded from being an object of personal property rights merely because it is digital or does not fall within the traditional categories of things in possession or things in action.

For India, the UK’s approach offers a useful point of reference. It demonstrates how statutory clarification of the legal status of digital assets can reduce uncertainty in an evolving regulatory landscape and provide a more predictable foundation for commercial, insolvency, and enforcement frameworks. More broadly, the Act reflects a global regulatory trend toward formalizing the legal standing of digital assets.

ESMA Issues MiCA Data Standards

In November 2025, the European Securities and Markets Authority (ESMA) issued further clarifications on the data, record-keeping, and reporting standards applicable under the Markets in Crypto-Assets Regulation (MiCA). The update forms part of MiCA's implementation phase and is aimed at ensuring consistent, enforcement-ready supervision of crypto-asset markets across the European Union.

Key requirements clarified by ESMA include:

- Standardized record-keeping obligations: Crypto-asset service providers (CASPs) must maintain harmonized records of services, orders, trades, and transactions to support supervisory review;
- Structured order-book data: Trading platforms are required to maintain granular, structured order-book data to enable detection of market abuse and manipulation;
- Uniform transparency standards: Pre- and post-trade transparency information must be provided in consistent, machine-readable formats to ensure comparability across Member States;
- Standardized crypto-asset white papers: ESMA has clarified format and content requirements for crypto-asset white papers, reinforcing comparable and analyzable investor disclosures; and
- Use of common identifiers: Where applicable, global identifiers (such as LEIs and token identifiers) must be used to support consistent classification and regulatory traceability.

ESMA has indicated that these standards are intended to support a smooth transition into MiCA's supervisory phase, with national competent authorities relying on harmonized data to enable cross-border monitoring, enforcement, and comparability across crypto-asset markets.

Canada Signals Stricter Regulatory Treatment of Stablecoins

In November 2025, the Bank of Canada reiterated its regulatory position on stablecoins that are capable of functioning as payment instruments. Canadian authorities have made clear that such stablecoins raise issues of monetary stability, consumer protection, and systemic risk, and should therefore be subject to safeguards comparable to those applied to payment and settlement instruments.

Regulatory signals emphasize expectations around full reserve backing, the use of high-quality liquid assets, and reliable redemption mechanisms to ensure stability and user confidence. As signaled in Canada's 2025 federal budget, the government intends to introduce a dedicated legislative framework governing fiat-backed stablecoins. The proposed approach would require stablecoin issuers to register with federal authorities, maintain one-to-one reserve backing with high-quality liquid assets, implement governance and risk-management safeguards, and comply with ongoing reporting obligations. In parallel, planned amendments to the Retail Payment Activities Act are expected to extend federal oversight to payment service providers handling stablecoin transactions, including custodial wallet and settlement services.

Taken together, these developments point to a gradual consolidation of stablecoin regulation at the federal level in Canada, with regulatory oversight increasingly anchored in payments, prudential, and financial-stability frameworks rather than fragmented or ad hoc crypto-specific measures.

Japan Tightens Supervisory Expectations for Crypto Asset Custody and Exchanges

In November 2025, Japanese financial regulators issued updated supervisory guidance clarifying expectations for crypto-asset exchanges and custodians operating under Japan's existing regulatory framework. The guidance reinforces requirements around asset segregation, custody safeguards, internal controls, and operational resilience, reflecting continued regulatory scrutiny of crypto market infrastructure.

The update emphasizes robust management of customer assets, clearer accountability for custody arrangements, and strengthened compliance and risk-management processes.

US Regulators Begin Implementing the GENIUS Act Stablecoin Framework

In December 2025, US regulators moved into the implementation phase of the GENIUS Act, initiating early rulemaking and inter-agency coordination to operationalize the federal framework for payment stablecoins. The focus of the initial steps is on translating statutory requirements into reserve, redemption, governance, and compliance obligations for stablecoin issuers.

The implementation process marks a shift from legislative adoption to practical regulation, with agencies expected to clarify supervisory responsibilities and reporting expectations in the months ahead.

Digital Assets / CLAUSE IN FOCUS

FORCE MAJEURE AND CYBER RISK IN CRYPTO CUSTODY AGREEMENTS

Force majeure clauses excuse performance where failures arise from events beyond a party’s reasonable control. In crypto custody arrangements between custodians and exchanges, banks, or funds, these clauses require careful drafting due to elevated cyber, operational, and theft risks. Exchanges typically seek to ensure that force majeure does not dilute the custodian’s fundamental obligations to maintain strong security and to return client assets, while custodians seek protection against genuinely external and uncontrollable disruptions. The central question is no longer whether a cyberattack occurred, but whether the incident was genuinely external and unavoidable despite the custodian having implemented appropriate security, governance, and resilience measures.

In recent regulatory and supervisory practice, force majeure carve-outs for cyber risk in crypto custody arrangements have continued to narrow. Reliance on force majeure for cyber incidents is now typically conditioned on evidence that the custodian acted in accordance with agreed security standards and that the disruption arose outside its reasonable sphere of control. Cyber incidents linked to internal systems, personnel, access controls, or governance failures are therefore less likely to qualify as force majeure, even if triggered by an external attacker. As a result, custodians can no longer rely on generic force majeure clauses to shield themselves from responsibility for cyber-related disruptions or asset losses arising within their systems or controls.

Draft Illustrative Clause

*“Neither Party shall be liable for delay or failure in performance resulting from events beyond its reasonable control (“**Force Majeure Event**”), including natural disasters, epidemics or pandemics, war, terrorism, government actions, or failure of public utilities, provided that a cyber or security incident shall constitute a Force Majeure Event only where it arises outside the Custodian’s reasonable control despite compliance with agreed cybersecurity, governance, and operational standards. The affected Party shall promptly notify the other Party and use reasonable efforts to resume performance. If such non-performance continues for more than sixty (60) days, the unaffected Party may terminate this Agreement upon written notice.*

For avoidance of doubt, a Force Majeure Event or termination shall not relieve either Party of its obligation to (i) pay any outstanding amounts, or (ii) return the Client’s crypto assets held in custody, in-specie and in trust.”

Negotiation Points

Exchange Perspective

- Any cyber-attack targeting the custodian's systems, infrastructure, or personnel is an operational failure and not a force majeure event.
- Right to appoint an external auditor to inspect and audit the custodian’s systems in the event of a force majeure event or any event impacting the exchange’s assets..
- In-specie asset return of exchange’s asset must survive force majeure and termination.
- Opposition to any “socialisation of losses” across the custodian’s clients.

Custodian Perspective

- Seek a clear carve-out for any losses resulting from the client's (exchange's) own negligence.
- Adequate time and operational flexibility to restore services post-event.
- Alignment of liability with agreed security standards rather than strict liability for all cyber outcomes.
- Clarification of the interaction between force majeure, insurance recoveries, and residual liability.

As crypto custody arrangements mature, force majeure clauses are increasingly used to define the boundary between operational responsibility and genuinely external disruption, rather than as broad liability shields. How cyber risk is carved out or preserved within these clauses now plays a central role in defining custody standards, accountability, and asset protection expectations.

Digital Assets

KNOWLEDGE CORNER

Centralized vs. Decentralized Exchanges

Centralized vs. Decentralized Exchanges

In the world of digital assets, the choice of trading platform carries significant legal and business implications. The fundamental distinction lies between Centralized Exchanges (CEXs), which operate like traditional financial intermediaries, and Decentralized Exchanges (DEXs), which facilitate direct peer-to-peer transactions through automated code. For businesses in India, the key difference boils down to regulatory clarity versus operational autonomy.

Centralized Exchanges (CEXs)

CEXs are privately operated entities that serve as trusted intermediaries, maintaining custody of users' assets and matching buy and sell orders through a centralized order book. This model delivers advantages such as deep liquidity, intuitive user interfaces, and essential fiat-to-crypto on-ramps.

From a regulatory perspective, CEXs may fall within India's existing legal framework. Further, a notification issued by the Ministry of Finance in March 2023 brought Virtual Digital Asset (VDA) service providers within the scope of the Prevention of Money Laundering Act, 2002 (PMLA). As a result, CEXs operating in India are classified as "reporting entities" and are required to register with the Financial Intelligence Unit–India (FIU-IND). This designation carries significant compliance obligations, including mandatory Know Your Customer (KYC) requirements, ongoing transaction monitoring, and the reporting of suspicious transactions. In addition, CEXs are responsible for deducting 1% tax deducted at source (TDS) on VDA transfers. For businesses, engagement with a CEX offers a high degree of regulatory clarity, albeit with inherent custodial risk, as asset custody is entrusted to the exchange.

Decentralized Exchanges (DEXs)

DEXs operate through blockchain-based smart contracts, allowing users to execute trades directly from their own non-custodial wallets without the involvement of an intermediary. This non-custodial architecture reduces exposure to exchange-level security breaches and supports greater user autonomy and privacy.

From a legal standpoint, DEXs presently exist in a regulatory grey area in India. Although no legislation expressly governs DEXs, the activity-based scope of the PMLA could, in theory, apply where a protocol is considered to facilitate transactions "for or on behalf of another person." In practice, however, the decentralized, automated, and leaderless nature of DEXs makes the enforcement of KYC, AML reporting, or TDS obligations extremely challenging. This regulatory ambiguity has led to concerns regarding the potential misuse of DEXs for illicit activities.

PART FOUR

DARK PATTERNS

FORCED ACTION

The Guidelines for Prevention and Regulation of Dark Patterns, 2023 define "Forced Action" as the practice of compelling users to perform an action that is not strictly necessary to access a product or service, such as mandating consent, sign-ups, or additional permissions as a precondition for use.

Common manifestations include:

❌ Mandatory account creation for basic browsing or price visibility

❌ Forcing users to accept marketing or data-sharing terms to complete a transaction

❌ Pre-ticked checkboxes for optional services or communications

❌ Requiring app permissions unrelated to core service delivery

Forced action is problematic not because platforms may impose legitimate conditions, but because compelled design choices blur the line between access and consent, undermining genuine user autonomy.

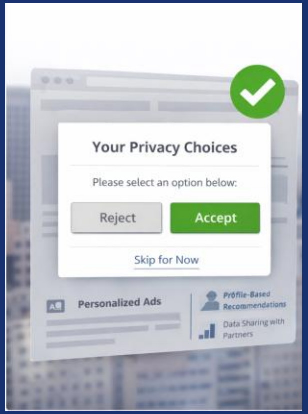
Better practice

✅ Limit mandatory actions to those strictly necessary for service delivery

✅ Ensure all optional consents require a separate, affirmative user action

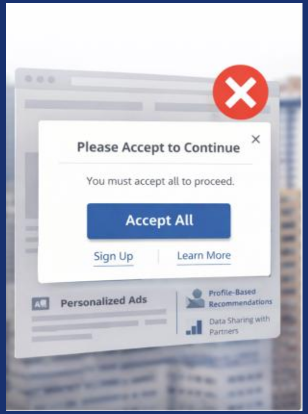
✅ Avoid default selections, pre-ticked boxes, or bundled permissions

✅ Clearly distinguish between core service access and optional features or communications



Your Privacy Choices

Please select an option below:



Please Accept to Continue

You must accept all to proceed.

Tip for businesses

Review onboarding, checkout, and permission flows to identify where users are compelled to act beyond what is necessary. Remove forced sign-ups, bundled consents, and default selections, and document design decisions to demonstrate that user actions reflect choice, not constraint.

BYTE/WISE

COMING SOON

JAN 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