MONTHLY EDITION – JANUARY 2026

FOUNTAINHEAD LEGAL

TECHNOLOGY LAW AND DATA PRIVACY UPDATES

INDEX

A. FOUNDER'S NOTES

B. NATIONAL UPDATES

- Government introduced stricter KYC/AML Framework for Crypto Platforms
- MeitY holds Stakeholder Consultations on Mobile Security Standards
- MeitY issued Notice to Social Media Giant over AI-generated Obscene and Non-Consensual Content
- Bombay High Court orders immediate Takedown of AI-generated Deepfake Content infringing Celebrity's Privacy
- Major Hotel Chain secures 'Sound Mark' Registration
- Delhi High Court lays down Framework on Fraudulent Domain Registrations
- CCPA penalizes Quick E-commerce Company for Dark Pattern Practices

C. INTERNATIONAL UPDATES

United States of America

- FTC hosts Virtual Workshop on Age Verification Technologies
- California's Delete Act enters into Force
- FTC appeals Ruling in Tech Giant Monopolization Case
- Government issues Request for Information on securing AI Agent Systems
- FTC updates Small Business Cybersecurity Guidance for Data Privacy Day

European Union

- EU grants Data Protection Adequacy to Brazil, easing Cross-Border Data Transfer Practice
- EC opens proceedings to ensure Tech Giant's Compliance under Digital Markets Regulation
- CJEU clarifies GDPR Transparency Obligations for Body-Worn Cameras and Observational Recording Tools
- EC publishes Summary of Consultation responses on Digital Markets Regulation Review
- EC signals Intent to Amend to Cybersecurity Directive
- France's National Assembly passed Bill to ban Social Media use for Children

United Kingdom

- Government strengthens Online Safety Regulation by prioritizing Cyberflashing Offences

Others

- Dubai modifies Crypto Token Regulatory Framework
- Vietnam's Personal Data Protection Law takes effect
- Singapore Privacy Authority penalises Travel Agency for Major Data Breach and Lapses in Accountability

D. ABBREVIATIONS

E. ABOUT FOUNTAINHEAD LEGAL & CONTACT DETAILS

FOUNDER'S NOTE

As January, anchored by International Data Privacy Day on January 28, 2026 has increasingly come to symbolise both reflection and action in the technology and data governance space. As 2026 begins, privacy and digital regulation are no longer confined to policy statements or future roadmaps. Across jurisdictions, regulators and courts are engaging directly with how digital systems function in practice, examining design choices, default settings, governance frameworks, and operational safeguards as concrete, enforceable compliance obligations.

Developments in India this month reflect this transition clearly. Stricter AML and KYC requirements for crypto platforms, judicial directions aimed at curbing anonymous and fraudulent domain registrations, and enforcement action against dark patterns in e-commerce point to a more coordinated and assertive regulatory approach. These measures signal an emphasis on accountability and transparency where digital systems intersect with consumer protection, financial integrity, and public trust.

These trends were also reflected in the Union Budget 2026, which reinforced the central role of digital infrastructure, cybersecurity resilience, and trusted data ecosystems in India's economic strategy. Long-term tax incentives for cloud and AI-driven infrastructure signal policy continuity and confidence in India's role as a global technology hub. At the same time, targeted initiatives promoting the use of artificial intelligence in agriculture highlight the Government's intent to deploy technology for inclusive, ground-level impact through data-driven decision-making, productivity enhancement, and risk mitigation for farmers. The Budget's focus on digital public infrastructure, fintech safeguards, and secure technology deployment underscores a clear policy recognition that economic growth and digital trust are deeply interconnected.

Globally, similar patterns are emerging. California's Delete Act has entered its enforcement phase, reshaping data broker compliance through centralised consumer controls, while antitrust scrutiny of dominant technology platforms continues in the United States. In the European Union, active supervision under the DMA, evolving cybersecurity frameworks, and judicial reinforcement of GDPR transparency obligations reflect regulatory maturity, where frameworks are tested, clarified, and refined through real-world application rather than constant legislative overhaul. Taken together, these developments point to a defining theme for 2026, technology regulation is no longer about anticipation alone, but about accountability in everyday digital operations.

We hope this edition captures that shift and provides readers with a clear view of how technology regulation is evolving, not just in statute books, but in its day-to-day application.

Rashmi,
Founder, Fountainhead Legal

NATIONAL

1. Government introduced stricter KYC/AML Framework for Crypto Platforms[1]

FIU-IND has issued *AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets* (**"Guidelines"**) mandating an enhanced KYC and AML framework for VDA service providers under the PMLA. Effective from January 8, 2026, the Guidelines introduce mandatory registration with FIU-IND as a pre-condition for operating as a VDA service provider, requiring entities to register on the FINgate portal, submit extensive organisational and technical documentation, and undergo an in-person compliance demonstration covering KYC systems, transaction monitoring, travel rule compliance, sanctions screening, and internal controls.

The Guidelines also significantly expand client due diligence, governance, and monitoring obligations. VDA service providers are now required to implement enhanced KYC measures (including PAN-based identification, liveness detection, geolocation and device data capture, and periodic KYC updates), appoint a Designated Director and Principal Officer, adopt Board-approved AML/CFT policies and risk assessments, and strengthen transaction monitoring and suspicious transaction reporting. Increased regulatory focus has also been placed on unhosted wallets, anonymity-enhancing tokens, mixers, and interactions with offshore or unregistered VDA platforms, alongside mandatory cybersecurity audits by CERT-In empanelled auditors. These changes materially raise the compliance threshold for crypto businesses in India and align VDA activities more closely with the regulatory expectations applicable to traditional financial institutions.

2. MeitY holds Stakeholder Consultations on Mobile Security Standards[2]

MeitY is holding stakeholder consultations on safety and security requirements applicable to mobile devices, as part of its ongoing engagement with industry on mobile security standards. The consultations cover a wide range of compliance parameters, including device safety norms, electromagnetic interference and compatibility requirements, interface standards, Indian language support, and security controls. These discussions form part of MeitY's broader efforts to review and strengthen regulatory expectations for mobile devices operating in India.

MeitY has indicated that the consultations are intended to inform the development of a structured and robust regulatory framework for mobile security, particularly in light of the growing reliance on smartphones for financial transactions, access to public services, and storage of sensitive personal data. Engagements with manufacturers and other stakeholders are also focused on understanding technical constraints, compliance costs, and

[1] https://fiuindia.gov.in/pdfs/downloads/VDA08012026.pdf
[2] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2213520&reg=3&lang=1

international best practices adopted across global markets, with a view to balancing security objectives with practical implementation considerations.

3. MeitY issued Notice to Social Media Giant over AI-generated Obscene and Non-Consensual Content[3]

On January 02, 2026, MeitY has issued a formal notice to the social media platform X Corp. ("**Company**"), raising concerns over the misuse of its AI chatbot 'Grok' to create and share obscene, sexually explicit, and non-consensual images. The Company has been directed to remove such content and submit a detailed 'Action Taken Report' outlining technical, procedural, and governance measures adopted to prevent further hosting, generation, or dissemination of obscene, vulgar, or unlawful material through the AI-enabled service. The notice emphasized that compliance with the IT Act and the IT Rules is mandatory, warning that non-adherence would be viewed seriously and could result in strict legal consequences.

The Company has acknowledged lapses in its content moderation and taken preliminary action by removing thousands of offensive Grok-generated items and deleting hundreds of accounts linked to their creation, while assuring authorities of stricter enforcement of platform policies. However, reports indicate that the Government was not fully satisfied with the company's initial response, noting a lack of detailed technical safeguards and proactive guardrails to prevent such misuse. The notice thus also sought a broader review of Grok's content generation mechanisms and safety guardrails to ensure alignment with India's digital content and intermediary liability framework.

4. Bombay High Court orders Immediate Takedown of AI-generated Deepfake Content infringing Celebrity's Privacy[4]

The Bombay High Court has directed the immediate removal of AI-generated deepfake content that infringed the privacy and dignity of actor Shilpa Shetty Kundra, underscoring judicial intolerance for non-consensual and harmful AI created imagery. In a petition filed in late 2025, the court observed that the circulation of sexually explicit deepfakes not only violated fundamental rights to privacy and dignity but also constituted a misuse of generative AI technology, meriting urgent judicial intervention. The court issued interim orders calling for takedown of the identified content across digital platforms and directed relevant intermediaries to disable access to such deepfakes pending final adjudication.

In reaching its decision, the court emphasized that AI generated deepfake content that depicts individuals without consent falls outside the ambit of protected expression and intrudes upon personal liberties guaranteed under the Constitution of India. It held that platforms and intermediaries have a corresponding duty to act expeditiously to prevent further dissemination once notified of such content.

---

[3] https://www.newsonair.gov.in/ministry-of-electronics-and-information-technology-issues-notice-to-x-seeking-removal-of-obscene-content/#:~:text=Transcript%20summary,misuse%20of%20AI%2Dbased%20services.

[4] Shilpa Shetty Kundra v. Getoutlive.in, 2025 SCC Online Bom 5486, Decided on 26-12-2025

The order reflects the judiciary's recognition of emerging harms facilitated by artificial intelligence and its willingness to apply existing legal doctrines of privacy, reputation, and intermediary liability to novel technological contexts.

5. Major Hotel Chain secures 'Sound Mark' Registration[5]

Taj Hotels (**"Taj"**), a luxury resort chain the Indian Hotels Company Limited, has successfully secured trademark registration for its distinctive sound mark, marking an important milestone in the evolution of non-traditional trademarks in India. A sound mark protects a unique audio identifier such as a signature tune or tonal sequence, that enables consumers to associate a sound directly with a brand, even in the absence of visual cues.

The registration grants Taj exclusive statutory rights over the use of the sound in relation to its hospitality services, strengthening its ability to prevent unauthorised imitation across advertising, digital platforms, and brand communications. This recognition reflects the Indian trademark regime's increasing openness to sensory branding, provided such marks meet the requirements of distinctiveness and identifiability under the Trade Marks Act, 1999.

This move underscores how sound is becoming a valuable commercial asset in an increasingly digital and experience-driven marketplace. For brands investing in experience-led marketing, this development underscores an important takeaway: distinctiveness today is no longer limited to visuals, and non-traditional trademarks are increasingly finding their place within the Indian legal framework.

6. Delhi High Court lays down Framework on Fraudulent Domain Registrations[6]

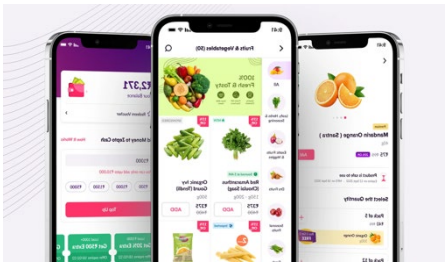
The Delhi High Court, while pronouncing its judgment in one of the matters, has issued a series of directions aimed at addressing the growing misuse of domain names deceptively similar to well-known brands by anonymous and unverified registrants. The case concerned the registration and operation of fake domain names used to impersonate legitimate businesses, mislead consumers, and facilitate fraud and trademark infringement. The court observed that the ease of anonymous domain registration had enabled large scale abuse, undermining consumer trust and brand protection in the digital ecosystem.

To curb such practices, the court directed domain name registrars to implement mandatory e-KYC based verification of registrant details, appoint grievance officers based in India, and share registrant information with law enforcement and regulatory authorities when required. It further ordered permanent blocking and suspension of fraudulent domains and permitted the grant of broader injunctions covering not only existing infringing domains but also future look alike registrations.

The ruling reflects a clear judicial shift toward holding domain name intermediaries more accountable for preventing online fraud and brand impersonation. While the directions impose additional compliance responsibilities on registrars, they are likely to strengthen trust in the domain name system and serve as an important deterrent against organised digital fraud and abuse of trademark rights.

[5] https://www.ihcltata.com/press-room/ihcl-secures-indias-first-sound-mark-registration-in-hospitality
[6] Dabur India Limited v. Ashok Kumar and Ors, CS (COMM) 135/2022 & I.A.s 3423/2022, 1221/2023 & 8858/2025

7. CCPA penalizes Quick E-commerce Company for Dark Pattern Practices[7]



CCPA has passed an order against Zepto Marketplace Pvt. Ltd. (**"Company"**) for engaging in unfair trade practices through the use of prohibited dark patterns on its platform. The CCPA found that the Company showed consumers a lower price at first, but added extra charges and pre-selected paid services only at the checkout stage, causing the final amount to be higher than expected. These practices were treated as dark patterns because the design of the checkout process nudged users into paying more without a clear and conscious choice. As a result, consumers were misled about the actual cost of their purchase and lost the ability to make an informed decision. CCPA further held that interface design choices, including color-coding and default selections, amounted to deceptive and manipulative practices in violation of the Consumer Protection Act, 2019, the Dark Pattern Guidelines, 2023, and the Legal Metrology (Packaged Commodities) Rules, 2011. While noting subsequent corrective steps taken by the Company, CCPA imposed a penalty of INR 7,00,000 and directed the Company to discontinue such practices, ensure upfront price transparency, and undertake regular self-audits to prevent recurrence.

While the penalty imposed is modest, the decision sends a clear compliance signal to e-commerce and quick-commerce platforms that manipulative interface design and opaque pricing practices will invite regulatory scrutiny, even if corrective steps are taken later. The order also aligns with a broader regulatory push across sectors, seen, for instance, in the Reserve Bank of India's digital lending guidelines, which similarly prohibit dark patterns and emphasise transparency, informed consent, and consumer trust, underscoring that fair design and upfront disclosures are fast becoming a cross-sector regulatory expectation rather than a platform-specific obligation.

[7] https://doca.gov.in/ccpa/checkuploaddocs.php?updocs=./uploads/1766468507-Zepto_Final_order__1___1_.pdf&unique_id=

INTERNATIONAL

UNITED STATES OF AMERICA

8. FTC hosts Virtual Workshop on Age Verification Technologies[8]

The FTC has hosted a virtual workshop on age verification technologies on January 28, 2026, bringing together regulators, industry representatives, consumer advocates, and academics to explore the use and implications of age verification and age estimation tools. The agenda included discussions on the regulatory landscape governing age assurance technologies, their intersection with the Children's Online Privacy Protection Act, 1998 and emerging compliance challenges for digital platforms. The workshop also explored technical approaches to age verification, privacy implications of different models, and the role of design choices in balancing child safety with data minimization.

Scheduled as an online-only event due to weather contingencies, the workshop reflected the FTC's ongoing focus on consumer protection in digital environments, especially where emerging technologies interact with children's privacy, platform safety, and compliance requirements. With this, FTC intended to foster dialogue on best practices, technical options, and potential policy considerations for regulating age verification technologies within existing legal frameworks.

While no immediate enforcement action or rulemaking has been announced, the initiative suggests that age assurance practices may face closer scrutiny in future consumer protection and privacy enforcement, particularly where platforms serve or target younger users.

9. California's Delete Act enters into Force[9]

California's Delete Act, 2023 is being rolled out in phases, giving both consumers and data brokers a clear compliance roadmap. From January 01, 2026, the Data Broker Registration and Opt-Out Platform (**"DROP"**) is live, allowing consumers to submit a single request to opt out of the sale or sharing of their personal data across all registered data brokers. For businesses, this marks the shift from policy to real-world enforcement.

The next milestones follow quickly includes Data brokers to complete annual registration by January 31, 2026, after which operational compliance kicks in from August 01, 2026. From this date, registered entities are expected to regularly access DROP (at least once every 45 days), act on consumer requests within prescribed timelines, and maintain auditable records of compliance. Looking ahead, the framework also introduces independent audit obligations from 2028 onwards, reinforcing long-term accountability. Together, these phased timelines signal that data broker regulation in California is no longer static but an ongoing, actively supervised compliance obligation.

[8] https://www.ftc.gov/news-events/news/press-releases/2026/01/ftc-host-virtual-workshop-january-28-age-verification-technologies

[9] https://privacy.ca.gov/drop/#:~:text=Step%201.,request%20for%20an%20elderly%20relative.

These developments highlight the need for data broking businesses to reassess their data practices, determine whether they meet the legal threshold of a data broker, ensure timely registration, and implement systems capable of responding to DROP-based deletion requests. With California shifting decisively from rulemaking to implementation, data brokerage activities are now subject to heightened regulatory visibility and enforcement risk.

10. FTC appeals Ruling in Tech Giant Monopolization Case[10]

FTC has filed a notice of appeal in January 2026 challenging the ruling by the U.S. District Court for the District of Columbia in its antitrust case alleging that Meta Platforms, Inc. ("**Meta**") maintained monopoly power in personal social networking services through anticompetitive acquisitions and conduct. At the core of the dispute is the FTC's allegation that Meta protected its dominance in personal social networking not by competing on the merits, but by systematically acquiring emerging rivals most notably Instagram and WhatsApp before they could grow into meaningful competitors. According to the FTC, this strategy reduced competitive pressure, limited consumer choice, and slowed innovation in social networking services. The appeal will now be heard by the U.S. Court of Appeals for the District of Columbia Circuit, reflecting the Commission's continued enforcement of U.S. competition law in digital markets.

By appealing the decision, the FTC is asking the U.S. Court of Appeals for the District of Columbia Circuit to revisit how monopoly power and competitive harm should be assessed in fast-moving digital markets. The appeal forms part of a broader federal effort to scrutinise concentration in the technology sector and to test whether long-term 'buy-or-bury' acquisition strategies by dominant platforms can amount to unlawful monopolisation. The outcome of this case could have significant implications for how antitrust law is applied to Big Tech and future acquisitions in digital ecosystems.

11. Government issues Request for Information on securing AI Agent Systems[11]

Centre for AI Standards and Innovation at National Institute of Standards and Technology ("**NIST**") issued a Request for Information ("**RFI**") on January 12, 2026 inviting input from AI developers, security researchers, and technology stakeholders on the unique security threats associated with autonomous AI agent systems. The RFI, published on NIST's official news portal, seeks examples of real-world attack vectors, risk mitigation techniques, and best practices for improving robustness and resilience of AI agents across deployment environments. The initiative is part of NIST's broader effort to anticipate and address emerging cybersecurity risks introduced by increasingly capable AI technologies.

The RFI recognizes that AI agent systems present distinct security concerns due to their ability to act independently, adapt to changing inputs, and interact with external systems. NIST has specifically invited feedback on vulnerabilities that may not be adequately addressed by traditional cybersecurity controls, as well as on governance and technical measures that could be incorporated at the design and

[10] https://www.ftc.gov/news-events/news/press-releases/2026/01/ftc-appeals-ruling-meta-monopolization-case
[11] https://www.nist.gov/news-events/news/2026/01/caisi-issues-request-information-about-securing-ai-agent-systems

deployment stages. The exercise is intended to support the development of informed guidance that reflects practical industry experience and evolving threat landscapes.

The request signals a proactive and anticipatory regulatory approach to AI security, focusing on risk identification before widespread deployment and enforcement. While the RFI does not impose binding obligations, it underscores growing federal attention on the security implications of agentic AI and suggests that future standards or guidelines may increasingly expect organizations to account for AI specific risks as part of broader cybersecurity and responsible AI governance frameworks.

12. FTC updates Small Business Cybersecurity Guidance for Data Privacy Day[12]

To mark Data Privacy Day on January 28 2026, the FTC updated '*Cybersecurity for Small Businesses'* (**"Cyber Guidance"**), its suite for small businesses providing guidance on cybersecurity risks and consumer data protection through its official business guidance platform. The Cyber Guidance highlights practical steps that small and medium sized businesses can take to mitigate common cyber threats such as phishing, ransomware, and unauthorized access to consumer data. It focuses on baseline security practices, employee awareness, incident preparedness, and responsible handling of personal information.

The FTC emphasized that small businesses are increasingly targeted by cybercriminals due to weaker security controls and limited resources, making cybersecurity awareness a critical component of consumer protection. By publishing updated Cyber Guidance, the agency aims to support businesses in adopting recognized security practices that reduce risk to both organizations and consumers. While the guidance does not introduce new legal obligations, it reflects the FTC's continued emphasis on reasonable security measures as a cornerstone of data protection compliance and also assists the small businesses in understanding the necessary or minimum requirements for preventing their systems from cyber threats.

[12] https://www.ftc.gov/business-guidance/blog/2026/01/recognize-data-privacy-day-protecting-your-small-business-cybercriminals

EUROPEAN UNION

13. EU grants Data Protection Adequacy to Brazil, easing Cross-Border Data Transfer Practice[13]

EC has recognized that Brazil's data protection framework provides a level of protection similar to that under the GDPR. This legal determination allows personal data to be transferred from the EU to Brazil without the need for additional transfer mechanisms such as standard contractual clauses, binding corporate rules, or supplementary safeguards.

This recognition is based on an assessment of Brazil's data protection law, regulatory oversight by its national data protection authority, enforcement powers, and the rights and remedies available to individuals. For businesses, this significantly reduces compliance complexity and legal uncertainty when working with Brazilian affiliates, vendors, or service providers handling EU personal data. More broadly, the decision reflects the EU's approach of facilitating international data flows with jurisdictions that demonstrate robust and enforceable privacy protections aligned with GDPR principles.

14. EC opens proceedings to ensure Tech Giant's Compliance under Digital Markets Regulation[14]

The EC has initiated formal proceedings to assist Alphabetic Inc. (**"Google"**) in complying with its obligations under the DMA, specifically in relation to interoperability and data sharing requirements. The proceedings focus on how Google enables access to online search data and interoperability for third-party services, which are central obligations imposed on designated 'gatekeepers' under the DMA.

This step is not a penalty action but a supervisory and compliance-focused measure, allowing the EC to clarify expectations, guide implementation, and monitor whether Google's technical and operational solutions meet DMA standards. The move underscores the EU's shift from rule-making to active oversight under the DMA, signalling that gatekeepers will be closely monitored not only for outright non-compliance, but also for how effectively they operationalise competition-enhancing obligations such as fair data access and interoperability in practice.

By stepping in early to guide interoperability and data-sharing compliance, the EC is signalling that the DMA is designed to actively re-engineer digital markets, not merely react to violations. For gatekeepers, this means regulatory oversight will extend deep into product design and technical implementation, making 'compliance by design' a commercial necessity rather than an afterthought.

[13] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_229

[14] https://digital-markets-act.ec.europa.eu/commission-opens-proceedings-assist-google-complying-interoperability-and-online-search-data-sharing-2026-01-27_en

15. CJEU clarifies GDPR Transparency Obligations for Body-Worn Cameras and Observational Recording Tools[15]

CJEU delivered an important ruling clarifying the scope of GDPR transparency obligations for organizations deploying body-worn cameras and other observational recording technologies. The case arose from the use of body-worn cameras in public-facing settings, where individuals were recorded automatically and continuously without direct interaction or individual notice. Complaints were raised on the ground that people captured on camera were often unaware that recording was taking place, who the controller was, or how their personal data would be used, given the passive nature of the surveillance and the absence of personalised disclosures. The dispute therefore centred on whether the practical difficulty of informing every individual in such environments could limit or relax the controller's transparency obligations under the GDPR, a question the court addressed by reaffirming that transparency remains mandatory, even in public and continuous monitoring contexts.

The court held that the use of such recording tools does not dilute an organization's duty to provide clear and accessible information to data subjects. Even where individual notice may be operationally challenging, controllers must adopt appropriate alternative measures, such as visible signage, layered privacy notices, or publicly available disclosures, to ensure individuals are adequately informed about the processing of their personal data.

From a compliance perspective, the ruling is significant for employers, security providers, public authorities, and private entities using surveillance or monitoring technologies. It reinforces that technological convenience or operational necessity cannot override the GDPR's transparency principle, and that organizations must proactively design accountability and notice mechanisms into the deployment of observational recording systems.

16. EC publishes Summary of Consultation responses on Digital Markets Regulation Review[16]

EC has published a summary and responses to the public consultation on the ongoing review of the DMA, fulfilling the legal requirement to review the regulation's effectiveness. The summary, released in early January 2026 via the commission's official portal, reflects broad participation with over 450 contributions from Member States, industry stakeholders, civil society, and SMEs. Respondents generally supported the DMA's objectives of fostering fair competition and reducing gatekeeper dominance, while many called for strengthened interoperability, data access, and broader scope including artificial intelligence and cloud services.

The consultation outcome will feed into the commission's formal review report due by May 03, 2026 to the European Parliament, the Council, and the European Economic and Social Committee. This phased review process, mandated under the DMA, seeks to ensure that the regulation continues to meet

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62024CC0422

[16] https://digital-markets-act.ec.europa.eu/commission-publishes-summary-and-responses-consultation-ongoing-review-digital-markets-act-2026-01-08_en

its goals in the rapidly evolving digital ecosystem, including the intersection of competition law with data and AI governance.

17. EC signals Intent to Amend to Cybersecurity Directive[17]

EC has signalled its intention to introduce targeted amendments to the National Information Systems (NIS) 2 Directive (**"NIS2"**), as part of its ongoing cybersecurity policy work. Announced in January 2026, the proposed changes are aimed at improving legal clarity and easing certain risk-management and compliance requirements, particularly for smaller organisations that fall within NIS2's scope while preserving strong cybersecurity obligations for operators of essential and important services.

NIS2 continues to serve as the backbone of the EU's framework for network and information systems security, setting out requirements on cybersecurity governance, incident reporting, and supervisory oversight. Since its adoption and transposition across Member States, stakeholders have raised concerns around interpretational complexity and uneven implementation. EC's proposed clarifications are intended to address these concerns by supporting more consistent application across Member States and reducing uncertainty around compliance expectations, without diluting NIS2's core cybersecurity objectives.

18. France's National Assembly passed Bill to ban Social Media use for Children[18]

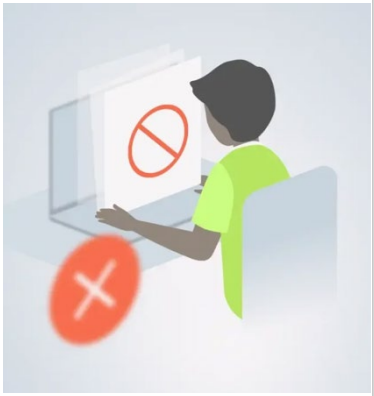
National Assembly has passed, *Proposition de loi, T.A. n° 217 (Bill aimed at protecting minors from risks associated with social network)* (**"Bill"**), that would ban children under the age of 15 years from accessing social media platforms, advancing a high-profile domestic policy initiative aimed at protecting minors from online harms. The Bill was adopted during a session on January 27, 2026, with broad parliamentary support, and is now expected to proceed to the Senate for final approval. The measures would require platforms to implement robust age verification systems and restrict accounts for younger users in line with the proposed age threshold, with enforcement deadlines aligned to the beginning of the 2026 school year.

From a legal and commercial perspective, the Bill signals a shift towards age-gated platform governance, with compliance consequences for social media and online service providers. Mandatory age-verification mechanisms, account restrictions, and school-year-linked enforcement timelines would require significant changes to onboarding flows, data processing practices, and user-experience design. For global platforms operating in France, this also raises broader questions around regulatory fragmentation, data minimisation in age verification, and the scalability of child-protection measures across jurisdictions.

[17] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[18] https://www.assemblee-nationale.fr/dyn/17/textes/l17t0217_texte-adopte-seance

UNITED KINGDOM

19. <u>Government strengthens Online Safety Regulation by prioritizing Cyberflashing Offences</u>[19]



The Government has amended the Online Safety Act, 2023 (**"OSA"**) to designate 'cyberflashing', the unsolicited sharing of nude or sexually explicit images, as a priority offence under the law, effective from January 8, 2026. Dating apps and social media platforms are now required to take proactive measures to prevent such content from appearing in users' feeds rather than merely responding after harm occurs. Platforms that fail to comply with the strengthened offence provisions may face fines of up to 10 per cent of global qualifying revenue or service blockage in the UK if they do not meet their obligations to protect users.

The change reflects the Government's broader online safety strategy aimed at protecting vulnerable users, particularly women and girls, from digital harms that undermine dignity and security. The Government indicated that regulators will consult on updated codes of practice to support compliance, reinforcing the OSA risk-based, harm-prevention framework.

[19] https://www.gov.uk/government/news/stronger-laws-for-tech-firms-to-ensure-you-dont-see-unsolicited-nudes

OTHERS

20. Dubai modifies Crypto Token Regulatory Framework[20]

The Dubai Financial Services Authority (**"DFSA"**) has implemented significant updates to its Crypto Token Regulatory Framework applicable in the Dubai International Financial Centre (**"DIFC"**). The revised framework introduces amendments across multiple Rulebook modules, including the Markets Rules (MKT), the Conduct of Business Rules (COB), the General Module (GEN), and the AML, CTF Module.

These modifications strengthen token admission and disclosure requirements, enhance market integrity and trading controls, impose clearer obligations around custody and safeguarding of client crypto assets, and tighten governance, risk management, and financial crime compliance obligations for regulated firms. The DFSA has also clarified expectations around client classification, suitability assessments, and technology controls, signalling a more supervisory-driven approach to crypto regulation in the DIFC. Collectively, these changes raise compliance standards for crypto businesses while providing greater regulatory clarity for firms operating within the DIFC.

21. Vietnam's Personal Data Protection Law takes effect[21]

Vietnam's Government enacted the Personal Data Protection Law ("**PDPL**") in June 2025 that officially came into force on January 1, 2026, establishing a comprehensive legal framework for safeguarding personal data in a rapidly digitalizing economy. The PDPL replaces earlier decree-level rules and significantly expands the scope of data protection obligations for both domestic and foreign entities that process personal data of Vietnamese residents.

It introduces detailed requirements relating to consent, classification of personal and sensitive data, cross-border transfer regimes, and mandatory impact assessments for high-risk processing activities, aligning the country's privacy standards with international norms. Further, organizations must implement enhanced operational safeguards, obtain clear and explicit consent for data processing, and adhere to stricter procedural controls for transfers and data subject rights. The PDPL also empowers authorities to impose substantial penalties for unlawful data trading and processing practices, including fines tied to illegal profits, emphasizing accountability across sectors such as finance, telecommunications, healthcare, and digital advertising.

The enactment of the PDPL marks a major milestone in Vietnam's digital regulatory regime by providing legal certainty for personal data protection and signaling the country's commitment to robust privacy governance as part of its broader digital economy strategy.

[20] https://www.dfsa.ae/news/dfsa-implements-major-updates-crypto-token-regulatory-framework-enhancing-market-integrity-and-supporting-innovation-difc

[21] https://vn.andersen.com/wp-content/uploads/2026/01/Laws-That-Entered-into-Force-as-of-1-January-2026.pdf

22. Singapore Privacy Authority penalises Travel Agency for Major Data Breach and Lapses in Accountability[22]

The Personal Data Protection Commission (**"PDPC"**) has fined Air Sino-Euro Associates Travel Pte. Ltd. (**"Company"**) SGD 47,000 following a cyber incident that exposed the personal data of more than 336,000 individuals. The breach involved unauthorized access to the Company's booking system, which stored extensive customer information, including identification documents and transaction records. The incident was uncovered after reports surfaced that stolen data had been accessed and shared online.

In its findings, the PDPC noted serious gaps in both data governance and technical safeguards. The Company had not put in place internal data protection processes, had failed to appoint a Data Protection Officer, and relied on outdated IT systems without adequate security controls such as multi-factor authentication or regular vulnerability reviews. PDPC also emphasized that engaging external IT vendors does not relieve organizations of their responsibility to oversee security and data protection measures.

Although the Company implemented corrective steps after the incident, the PDPC made it clear that remediation after a breach cannot substitute for baseline compliance. The decision serves as a reminder that organizations handling large volumes of sensitive personal data must embed accountability and security into day-to-day operations, particularly where legacy systems and third-party vendors are involved.

[22] https://www.pdpc.gov.sg/all-commissions-decisions/2026/01/breach-of-the-accountability-and-protection-obligations-by-air-sino-euro-associates-travel-pte-ltd

ABBREVIATIONS

AI – Artificial Intelligence

AML – Anti-Money Laundering

CCPA – Central Consumer Protection Authority

CERT-In – Computer Emergency Response Team - India

CFT – Combating the Financing of Terrorism

COPPA – Children's Online Privacy Protection Act.

DMA – Direct Marketing Association

EC – European Commission

ED – Enforcement Directorate

FIU-IND – Financial Intelligence Unit - India

FTC – Federal Trade Commission.

GDPR – General Data Protection Regulation

IT Act – Information Technology Act, 2000

IT Rules – The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

KYC – Know Your Customer

MeitY – Ministry of Electronics and Information Technology

PMLA – Prevention of Money Laundering Act, 2002

SMEs – Small and Medium-sized Enterprises

VDA – Virtual Digital Assets

ABOUT FOUNTAINHEAD LEGAL

Fountainhead Legal is an emerging law firm specializing in key practice areas of data privacy & technology law, indirect taxation and general corporate law. The firm's team of experienced and dynamic young lawyers blends deep legal expertise with fresh perspectives, delivering innovative, solution-oriented legal counsel. This synergy of knowledge and energy ensures clients receive forward-thinking advice tailored to their unique needs. The firm's services include drafting privacy policies, offering expert opinions on data privacy and security practices, and developing robust compliance frameworks. Fountainhead Legal has been instrumental in keeping organizations ahead of evolving regulatory requirements by providing regular updates and expert guidance.

We are committed to supporting organizations on this journey. With our deep expertise in data privacy compliance and a strong understanding of regulatory nuances, we offer tailored solutions for each client's unique needs. From drafting privacy policies and developing data protection frameworks to advising on cross-border data transfers and facilitating employee training programs, our team is equipped to guide clients through every stage of their compliance strategy.

Rashmi Deshpande, the founder of Fountainhead Legal, is a seasoned professional with close to 20 years of experience with Big 4 consulting and law firm. She has worked at Deloitte, BMR & Associates, KPMG, and PwC, and was a partner at Khaitan & Co. before founding Fountainhead Legal in 2023. Her practice encompasses data privacy, general corporate advisory, contract drafting, and litigation management, with expertise across industries such as financial services, fintech, insurance, IT/ITES, life sciences, and real estate. Rashmi is well-versed in data privacy regulations, including India's DPDP Act and GDPR, assisting clients in navigating compliance, drafting privacy policies, and establishing robust data protection frameworks.

Aarushi Ghai, senior associate, is a law graduate from NMIMS University, is a dedicated legal professional specializing in Data Privacy, Technology Law, Indirect Tax, and General Corporate matters. She advises businesses across sectors on regulatory compliance and strategic legal solutions. She has guided fintech clients on data deletion challenges, privacy policies, and software agreements, leveraging her expertise in India's DPDP Act and global privacy laws to build strong data governance frameworks.

Vaibhav Gupta, associate, is a legal professional with over two years of experience in litigation and corporate advisory. He holds an LL.M. in Technology Law from the National University of Juridical Sciences, Kolkata. His practice focuses on technology law, data privacy, and litigation management, advising clients on regulatory compliance under the technology and data privacy regulations. Vaibhav assists businesses in navigating privacy obligations and legal risks in the evolving digital ecosystem.

Dr. (Lt Col) G. U. Deshpande, MD (Path), DCP, FICP, is a highly respected Consultant in Histopathology and Laboratory Medicine with nearly five decades of experience. As an Advisor to Fountainhead Legal, he brings deep expertise in medico-legal matters, data privacy in hospital administration, and legal cases involving the Armed Forces. A distinguished alumnus of AFMC, Pune, and a recipient of several national awards for medical research, Dr. Deshpande has held prominent academic and clinical roles, including long-standing teaching tenures and leadership at his own diagnostic centre in Pune. His multifaceted background allows him to offer a unique and valuable perspective at the intersection of medicine, law, and data governance.

CONTACT DETAILS

Rashmi Deshpande
Email: rashmi@fountainheadlegal.com
Contact Number: +91 98338 62234
LinkedIn: https://www.linkedin.com/in/rashmi-deshpande-3775b336/

Aarushi Ghai
Email: aarushi@fountainheadlegal.com
Contact Number: +91 91314 15290
LinkedIn: https://www.linkedin.com/in/aarushi-ghai-282130179/

Vaibhav Gupta
Email: vaibhav@fountainheadlegal.com
Contact Number: +91 77987 96778
LinkedIn: https://www.linkedin.com/in/vaibhavguptav21/

Address
C - 2106, Oberoi Garden Estate,
Chandivali Farm Road, Powai – 400 072

Website: https://fountainheadlegal.com/
LinkedIn: https://www.linkedin.com/company/fountainhead-legal/