FOUNTAINHEAD LEGAL

FOUNTAINHEAD LEGAL

TECHNOLOGY & DATA PRIVACY BULLETIN

Insights on Technology Law, Data Protection & Digital Governance

IN INDIA	US UNITED STATES	EU EUROPEAN UNION	OTHERS

MONTHLY EDITION **[MAY 2026]**

FROM THE DESK OF OUR FOUNDER

FOUNDER'S NOTE

This month marks a noticeable shift in the AI governance conversation. For the past two years, the focus has largely been on principles, frameworks, and future regulation. May felt different. Across jurisdictions, governments, regulators, and courts began answering a more practical question: who is responsible when AI systems are deployed, and how should that responsibility be enforced?

In the United States, the long-running debate over whether AI should be governed through a single federal framework or through state-level legislation became more pronounced. Connecticut and Colorado both advanced significant AI-related laws with bipartisan support, signalling that states are not waiting for a national consensus before acting. Much like privacy regulation before it, AI governance is beginning to develop along parallel federal and state tracks.

In India, the focus has shifted from legislation to implementation. MeitY's call for applications for the Chairperson and Members of the Data Protection Board is a reminder that the Digital Personal Data Protection Act is moving steadily toward enforcement. Alongside this, judicial and regulatory developments from gaming restrictions to cybersecurity advisories referencing specific AI tools, reflect institutions gradually building the mechanisms through which compliance expectations will be enforced. Businesses that have assumed a slow regulatory rollout may need to revisit those assumptions.

Europe offered a different lesson. While the EU's Digital Omnibus package eases certain compliance burdens and extends timelines for some AI Act obligations, it also introduces new and more targeted requirements. The result is not deregulation, but a more nuanced regulatory landscape with multiple compliance deadlines running simultaneously. For organisations operating AI systems in Europe, understanding which obligations apply and when may become just as important as understanding the obligations themselves.

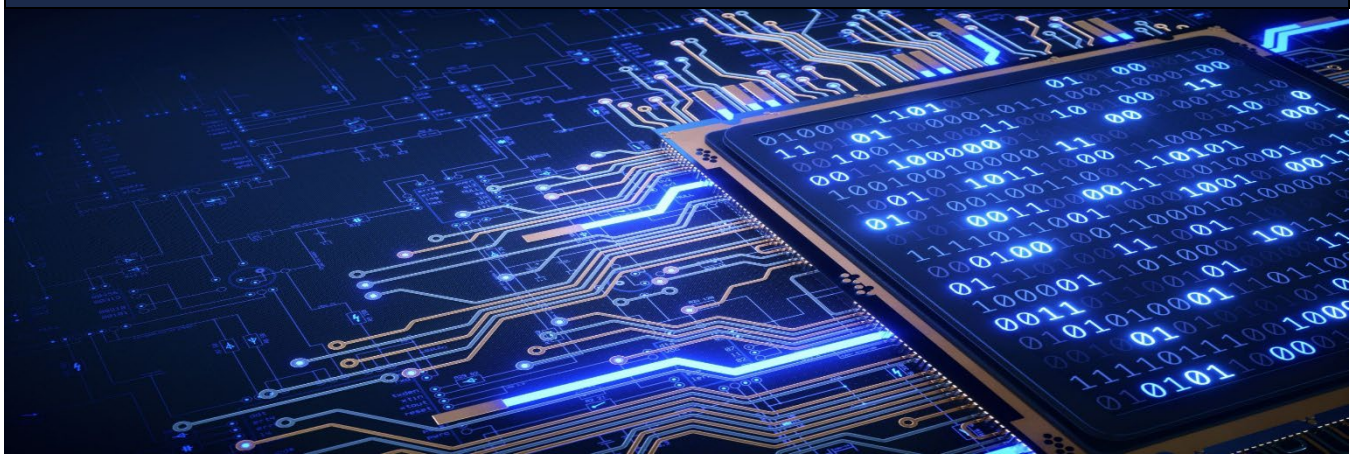
Several other developments reinforce a broader trend. China has begun treating agentic AI as a distinct regulatory category. Japan is strengthening enforcement powers under its privacy framework. Courts in both the United States and China are being asked to address questions of liability, workplace impact, and accountability arising from AI deployment. Together, these developments highlight an important reality: the legal risks associated with AI now extend far beyond privacy and data protection. Employment law, product liability, consumer protection, platform regulation, and cybersecurity are increasingly becoming part of the same conversation.
The message from May is clear. The era of preparing for AI regulation is gradually giving way to the era of operating within it. Organisations are no longer being asked whether they use AI. They are being asked whether they can demonstrate governance, accountability, and oversight over the systems they deploy.

With that context, we hope you find this month's updates insightful!

IN THIS ISSUE

TABLE OF CONTENT

| INDIA



1	**Government invited Applications for Data Protection Board of India**[1] MeitY has initiated the process to appoint the Chairperson and Members of the DPBI, constituted under the DPDP Regulations. The DPBI has been envisaged as a completely digital, paperless adjudicatory body responsible for investigating personal data breaches, assessing compliance with the DPDP Regulations, and imposing monetary penalties. Applications have been invited for one chairperson, requiring experience equivalent to an Additional Secretary rank in the Government, and four members, requiring experience at the level of Joint Secretary or equivalent in government, industry, or academia, with at least one member mandated to hold expertise in law. Appointments carry fixed tenures of up to 2 years or until the age of 65, whichever is earlier, and applicants must be at least 55 years old at the time of application. *This is a significant operational step in India's data protection journey since the notification of the Rules under DPDP Regulations. With the DPBI's constitution now actively underway, the compliance obligations under the DPDP Regulations transition from statutory text to enforceable reality. Organizations that have deferred readiness on the assumption that enforcement is distant now face a changed calculus. The appointment process, once concluded, will set the stage for the DPBI to begin hearing complaints and adjudicating disputes, making the question of institutional readiness a live one.*
2	**Supreme Court upheld State Laws banning Online Real-Money Gaming**[2] In a landmark judgment, Supreme Court upheld the constitutional validity of state laws enacted by the States of Tamil Nadu and Karnataka that criminalise online games played for money or stakes, including rummy, poker, and fantasy sports. The court held that there is no fundamental right to engage in betting and gambling. Such activities fall outside the domain of ordinary commercial protection under the Constitution of India, meaning they cannot claim the same protections as legitimate trade or business. The court also clarified that once real money is staked on a game, whether the game is skill-based or chance-based no longer matters for the purpose of state regulation. States were accordingly held to retain the power to regulate or prohibit even skill-based games if played for money, and the court upheld, in a separate judgment, the levy of 28% GST on online gaming bets.

[1] https://www.meity.gov.in/static/uploads/2026/05/cd481c027470b420b4cb85fb40a91c53.pdf, accessed on May 28,2026.
[2] State of Tamil Nadu & Ors. v. Junglee Games India Pvt. Ltd. & Anr., C.A. No. 6124-6131/2023.

Given that the ruling interprets foundational concepts of gaming, betting, and gambling, it bears directly on the ongoing constitutional challenge to the PROGA. The ruling strengthens the legal architecture on which both state gaming laws and the central PROGA framework rest. For gaming platforms, real-money game operators, and intermediaries, the judgment confirms that courts are unlikely to be receptive to skill-game arguments where monetary stakes are involved.

3 **RBI proposed Draft Rules to block Loan-Default Phones remotely**[3]

RBI released the second draft of the *Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Amendment Directions, 2026* **("Draft Directions")**, and kept open for stakeholder comments till May 31, 2026. Post closure of this deadline the Draft Directions are proposed to take effect from October 1, 2026. The Draft Directions propose that regulated lenders may remotely restrict certain functionalities of a mobile phone or tablet financed through a loan from that lender, but only after the loan becomes 90 days past due. However, such action should follow a staged notice process: a notice after 60 days past due allowing 21 days to repay followed by a second notice allowing at least a further 7 days. The consent of the borrower must have been obtained in the loan agreement. Essential services including internet access, incoming calls, emergency SOS features, and Government notifications may not be blocked.

Lenders are also prohibited from accessing personal data stored on the device and from using device restriction technology for personal, car, or home loans, confining the mechanism strictly to device-financing loans. Broader recovery conduct norms are also tightened, including restriction of contact timings to 8 a.m. to 7 p.m., prohibition on threatening or abusive language, and mandatory call recording for at least 6 months.

The proposed framework attempts to balance recovery rights with privacy interests by restricting access to personal data even where device functionality may be remotely controlled. Lenders and technology providers will need to ensure that device restriction tools operate without collecting, viewing, or processing personal data, particularly in light of increasing scrutiny under the DPDP regime.

4 **SEBI issued Advisory on AI-driven Cybersecurity Risks**[4]

SEBI issued the *Advisory on Emerging Advanced Artificial Intelligence (AI) Tools for Vulnerability Detection* **("Advisory")**, specifically naming 'Claude Mythos' as an example of advanced AI tools capable of scanning applications and networks to detect vulnerabilities at significant scale and speed. This raise concerns around data confidentiality, application integrity, and reliability of AI-generated outputs. A breach at any one participant can cascade across the interconnected securities market ecosystem. In response, SEBI has constituted a dedicated task force, cyber-suraksha.ai, to assess the evolving threat landscape.

Regulated entities have been directed to strengthen API security, enhance monitoring through Security Operations Centres ("**SOC**"), conduct continuous AI-related risk assessments, ensure timely patching, and onboard to the Market-SOC framework. Vendor oversight for AI-related security scenarios is also required. Exchanges and depositories must additionally require their empanelled application vendors to conduct comprehensive risk assessments covering AI-driven vulnerability detection models.

If you are a SEBI-regulated entity using or procuring AI tools, this Advisory creates immediate action items from SOC enhancements to vendor risk assessments.

[3] https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=62776, accessed on May 30,2026.
[4] https://www.sebi.gov.in/legal/circulars/may-2026/advisory-on-emerging-advanced-artificial-intelligence-ai-tools-for-vulnerability-detection_101270.html, accessed on May 28,2026.

5 **Industrial Relations (Central) Rules, 2026 notified**[5]

The Ministry of Labour and Employment notified the *Industrial Relations (Central) Rules, 2026* ("**IR Rules**") with effect from May 8, 2026, under the Industrial Relations Code, 2020. Key requirements include formation of Grievance Redressal Committees for establishments with 20 or more workers, structured procedures for recognising negotiating unions, formalised fixed-term employment provisions on par with permanent workers, and mandatory electronic record-keeping and digital filing.

The IR Rules apply to sectors where the Central Government is the appropriate government, including banking, insurance, telecommunications, civil aviation, railways, mines, oil fields, and central public sector enterprises.

For businesses in these sectors, the IR Rules introduce a more documentation-intensive and digitally driven compliance environment. Notably, the shift to electronic record-keeping intersects with DPDP Regulations compliance, since employment records contain personal data of workers and must now be maintained in digitally accessible formats.

6 **CERT-In released Blueprint for Defending against AI-Assisted Cyber Threats**[6]

CERT-In published *Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure* **("Blueprint")**, establishing India's most specific expectations to date on the speed of vulnerability remediation. The Blueprint responds to CERT-In's assessment that threat actors are increasingly using generative AI, large language models, and autonomous agentic systems to accelerate gathering of information, exploit development, and large-scale attack.

The Blueprint sets a tiered remediation schedule: known exploited vulnerabilities on internet-facing and critical systems must be patched, mitigated, or isolated within 12 hours where feasible. Critical externally exposed vulnerabilities within one day, critical internal vulnerabilities on high-value systems within three days and high-severity vulnerabilities within five days. The Blueprint also introduces a three-phase, 60-day implementation roadmap spanning governance, monitoring, AI governance, and supply chain assurance.

The 12-hour patching window for critical internet-facing vulnerabilities is aggressive. Organizations that do not have automated patch management and continuous monitoring in place need to act immediately.

7 **Supreme Court directed MeitY to examine PIL on Stolen Personal Data**[7]

The Supreme Court has declined to directly hear a PIL filed by a cybersecurity consultant seeking judicial intervention to recover or destroy stolen personal data of Indian citizens allegedly held on servers across multiple foreign countries. The PIL flagged serious concerns over the misuse of sensitive identifiers, including fingerprints and biometric data, for transnational cybercrime, digital arrests, and extortion. The petitioner also sought directions to operationalise the DPDP Regulations. The court observed that the issues were predominantly technical and administrative in nature, not warranting judicial intervention at this stage, and directed the petitioner to submit the petition as a formal representation to MeitY for examination.

The court's direction carries meaningful policy significance. It signals that cross-border theft and misuse of personal data is being acknowledged at the highest levels and must be addressed through administrative and technological expertise. The referral places the matter squarely within the ambit of executive and regulatory action.

[5] https://egazette.gov.in/WriteReadData/2026/272336.pdf , accessed on May 28,2026.
[6] https://www.cert-in.org.in/PDF/Blueprint_for_Defending_against_AI_Assisted_Exploitataion.pdf, accessed on May 30,2026.
[7] Nitish Kumar v. Union of India [W.P.(Crl.) No. 163/2026]

This may prove consequential in shaping how the DPDP Regulations is operationalised, particularly regarding cross-border breach scenarios, remediation mechanisms, and India's ability to assert data sovereignty when citizen data is compromised beyond its territorial jurisdiction.

8 **PIL before Supreme Court on Restricting use of Aadhaar**[8]

A PIL has been filed before the Supreme Court under Article 32 of the Constitution of India, seeking directions to the Union Government, State Governments, and the Election Commission of India to restrict the use of Aadhaar strictly to identity verification. The PIL contends that Aadhaar as clarified under the Aadhaar Act, 2016 and UIDAI notifications, is not a document of citizenship, domicile, residential address, or date of birth. Despite this, it is being routinely accepted for these purposes across school admissions, property transactions, voter registration, ration cards, driving licences, and birth certificates. The petitioner has sought a declaration that the use of Aadhaar as proof of date of birth and residence in voter registration forms is unconstitutional and void.

The PIL also called for stronger digital verification safeguards including a high-powered monitoring committee comprising a retired Supreme Court judge and technical experts. The PIL raises systemic questions about scope creep in the use of Aadhaar beyond its statutory purpose. Similar concerns have featured in earlier jurisprudence including the nine-judge bench decision in K.S. Puttaswamy[9] though in a different regulatory context. The court disposed of the writ petition directing Union of India to examine the petitioner's representation and communicate its decision within 2 months. All contentions on merit were kept open.

9 **Delhi High Court flagged AI Use in Trial Court Judgment in Akasa Air Dispute**[10]

The Delhi High Court flagged serious concerns over the possible use of AI tools in drafting a Commercial Court judgment. The case arose from a decree awarding INR 1,08,80,000 to a tour operator against Akasa Air in respect of 640 airline tickets. SNV Aviation Private Limited **("Akasa Air")** challenged the decree on two grounds. First, the decree contained references to non-existent propositions of law falsely attributed to Supreme Court precedents. Second, the award of the entire ticket cost as lost profits was legally untenable.

On prima facie examination, the court noted that there was an impression that AI tools may have been used in drafting, while expressly refraining from making a conclusive finding. It also left open whether the judgment had been duly reviewed thereafter. The decree was stayed subject to a deposit of INR 20 lakhs by Akasa Air, with the matter listed for August 20, 2026.

10 **ASCI released Draft Guidelines on AI-generated Content Labelling in Advertising**[11]

The Advertising Standards Council of India **("ASCI")** released *Draft Guidelines for Responsible Labelling of Synthetically Generated Content in Advertising* **("Draft Guidelines")**, open for public consultation until June 13, 2026. The Draft Guidelines are aligned with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 **("IT Amendment Rules")** and adopt a risk-based approach that classifies AI use in advertising into three categories. High-risk content is prohibited outright, regardless of disclosure. This includes fabricated endorsements, deepfakes, exaggerated claims, AI-generated authority figures such as fake doctors, and use of a person's likeness without consent. Such content constitutes a violation of the ASCI Code even if labelled.

[8] Ashwini Kumar Upadhyay v. Union of India, Writ Petition(s)(Civil) No.590/2026.
[9] Justice K.S. Puttaswamy (Retd) v. Union of India, Writ Petition (Civil) No. 494 OF 2012.
[10] SNV Aviation Pvt. Ltd v. ABS Tour and Travels, RFA(COMM)284/2026, Delhi High Court.
[11] https://www.ascionline.in/wp-content/uploads/2026/05/asci-ai-labelling-guidelines.pdf, accessed on May 28, 2026.

Medium-risk content, such as virtual influencers or entirely AI-generated realistic scenarios, requires mandatory labelling through standard disclosures such as "Audio/Video created using AI" or "Audio/Video enhanced using AI". Low-risk uses, including routine colour correction, ambient music, fantastical elements, or administrative content generation, do not require labelling.

The Draft Guidelines further clarify that where disclosures are required, they must comply with ASCI's existing disclaimer guidelines. These are intended to operate alongside, and not independently of, the obligations already embedded in the IT Amendment Rules.

11 **TRAI released Consultation Paper on Vehicle-to-Everything Communication Framework**[12]

TRAI released a *Consultation Paper on the Regulatory Framework for Vehicle-to-Everything Communication* **("V2X") ("Consultation Paper")** at the request of the Department of Telecommunications. V2X is a wireless technology enabling vehicles to exchange real-time data with other vehicles, road infrastructure, pedestrians, and mobile networks, with significant implications for road safety, traffic management, and autonomous driving.

The Consultation Paper identified Cellular V2X over 4G and 5G networks as the preferred approach and sought stakeholder feedback on spectrum allocation, technology standards, and issues relating to data ownership, privacy, and liability. To address privacy concerns, TRAI proposed mechanisms that would allow vehicles to be authenticated while protecting the identity of drivers and users. Comments were invited until May 28, 2026, with counter-comments due by June 11, 2026.

The Consultation Paper highlights that connected vehicles will not just be a transportation issue, but also a data protection issue. To the extent vehicle-generated data can identify or be linked to a driver, it may constitute personal data under the DPDP framework, making compliance with data protection obligations an important consideration for automotive, mobility, and telecom stakeholders.

12 **Supreme Court ordered location tracking and panic buttons in Public Service Vehicles**[13]

While dealing with a PIL concerning road safety and implementation of the Motor Vehicles regulations, the Supreme Court reviewed compliance with various safety measures mandated under the Central Motor Vehicles Rules, 1989 (**"CMV Rules"**). During the proceedings, the court was informed that compliance with Rule 125H, which requires Vehicle Location Tracking Devices (**"VLTDs"**) and panic buttons in public service vehicles, remained extremely low, with less than 1% of transport vehicles reportedly equipped with VLTDs.

Accordingly, the court directed all States and UTs to strictly enforce Rule 125H of CMV Rules requiring installation of VLTD and panic buttons in all public service vehicles, including taxis. It further directed that no public service vehicle may be granted a fitness certificate or transport permit unless it is fitted with both devices. The court also endorsed the proposal that manufacturers install these features at the manufacturing stage itself, directing the Central Government to consult automobile manufacturers and submit a feasibility report.

The court separately noted that the National Road Safety Board had not yet been constituted despite prior directions and a last opportunity of 3 months, and criticised multiple States for non-compliance with speed governor reporting requirements.

The directions carry immediate compliance implications for fleet operators, taxi aggregators, and vehicle manufacturers. Further, this is another example of technology being embedded into regulatory and public infrastructure frameworks. While such measures can improve safety and accountability, they

[12] https://trai.gov.in/sites/default/files/2026-04/CP_30042026.pdf, accessed on May 28, 2026.
[13] S. Rajaseekaran v. Union of India, W.P. (C) No. 295/2012.

also result in the collection of large volumes of location and behavioural data, making robust data governance and compliance with emerging privacy obligations critical.

13 **Tamil Nadu and Kerala formed Dedicated AI Portfolios at Cabinet Level**

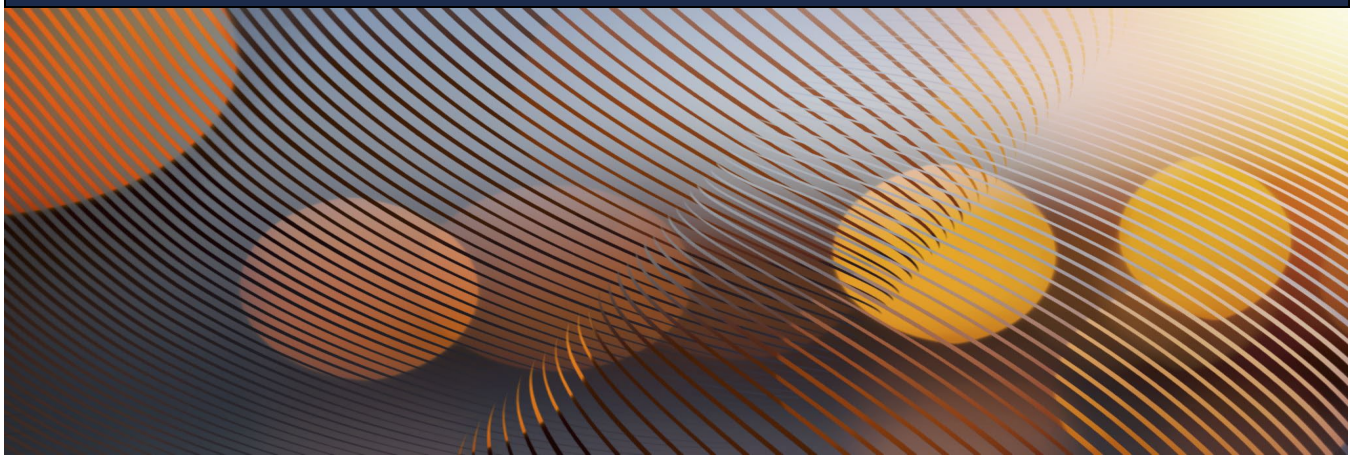
Tamil Nadu created a dedicated portfolio for AI[14], combining it with the existing IT and Digital Services Ministry. The AI portfolio has been assigned to a cabinet minister and is aligned with the state government's agenda of integrating AI into public service delivery, promoting AI innovation infrastructure, and supporting deep-tech startups.

Kerala went a step further by becoming the first state in India to create a dedicated AI portfolio at the cabinet level[15]. Following the formation of the new state cabinet, the General Administration (Protocol) Department issued a notification formally allocating ministerial portfolios. As part of this allocation, AI was explicitly named as a distinct and separate portfolio designation within a combined ministerial assignment. Unlike Tamil Nadu, where AI was merged with the existing IT and Digital Services Ministry, Kerala's approach reflects a more pronounced structural commitment to AI governance at the highest level of executive decision-making.

State-level AI governance is becoming institutionalised. Businesses deploying AI in public services or seeking state partnerships should engage early with these new ministries. Policy frameworks, procurement preferences, and regulatory expectations will increasingly be shaped at the state level.

[14] https://lokbhavan.tn.gov.in/lok-bhavan-press-release-no-40-dated-21-05-2026/ , accessed on May 30, 2026.
[15] http://www.niyamasabha.org/codes/cmin-new.htm , accessed on May 30, 2026.

| UNITED STATES OF AMERICA



14	**FTC settled with Location Data Broker, banning Sale of Sensitive Location Data**[16] FTC announced a proposed stipulated final order resolving its enforcement action against data broker Kochava Inc. **("Kochava")** and its subsidiary Collective Data Solutions LLC. The FTC had filed suit in August 2022 alleging that Kochava sold precise geolocation data linked to hundreds of millions of mobile devices in ways that exposed users' movements to sensitive locations, including reproductive health clinics, places of worship, and domestic violence shelters, without their knowledge or consent. The proposed order prohibits Kochava and its subsidiary from selling, sharing, or disclosing sensitive precise location data unless the consumer has provided affirmative express consent tied specifically to a service they have directly requested. The order is subject to court approval before becoming binding. Additional obligations include establishing a programme to identify and manage sensitive locations within data held, implementing a supplier assessment programme to confirm that third-party data carries proper consumer consent, allowing individuals to request the names of parties to whom their location data was disclosed, and deleting data on a defined schedule rather than retaining it indefinitely. *Consent is becoming a supply-chain issue. Regulators are increasingly requiring organisations to validate the provenance of data, assess whether appropriate permissions exist, and maintain accountability across downstream disclosures. The focus is shifting from collecting consent to demonstrating that consent remains effective throughout the lifecycle of the data. Businesses can no longer assume that data obtained from third parties is compliant by default.*

15	**Connecticut passed AI Responsibility and Transparency Act**[17] The House of Representatives passed the *Connecticut Artificial Intelligence Responsibility and Transparency Act* **("AI Act")**. The Governor indicated his intent to sign the bill, which attracted bipartisan support in both chambers. AI Act spans a range obligations, including employment-related automated decision-making and AI use within state agencies and a state-managed regulatory sandbox for testing new AI technologies and products. It also incorporates provisions on youth social media use and interactions with AI chatbots, and includes AI literacy programmes and AI education support for small

[16] Federal Trade Commission v. Kochava Inc., Case No. 2:22-cv-00377-BLW.
[17] https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2026&bill_num=5, accessed on May 28,2026.

businesses. A companion bill on consumer data privacy, *Senate Bill 4*, is expected to come up for a vote separately and may add further obligations for businesses operating in the state.

The passage of the AI Act is significant in its wider context. Connecticut joins a growing number of states legislating on AI even as the federal administration has sought to discourage state-level action in favour of a single national standard.

16 **Colorado enacted Age Attestation Law for Computing Devices**[18]

The legislature passed Senate Bill 26-051 titled *Concerning Age Attestation for Users of Computing Devices* **("SB 51")**, creating an obligation for operating system providers to implement an accessible interface at account setup through which the account holder indicates the birth date or age of the device user, generating an age bracket signal that must be made available in real time to application developers on request.

Developers of applications available through covered app stores are required to request this age signal for each user download and are deemed to have knowledge of the user's age range once the signal is received, across all platforms and points of access of the application. Neither operating system providers nor developers may share the age signal with third parties for any purpose not required under SB 51. Violations carry civil penalties of up to USD 2,500 per minor affected by a negligent violation and up to USD 7,500 per minor affected by an intentional violation, enforceable by the attorney general. The compliance implementation date is July 1, 2028.

This marks a meaningful shift in how age assurance is approached in digital services. Rather than placing the burden on individual platforms through self-declaration or platform-specific verification, it embeds age determination into operating system-level infrastructure. This creates a more consistent and structurally reliable mechanism across all platforms and points of access.

17 **AI Research Organization sued over its LLM advice**[19]

A complaint was filed in the San Francisco Superior Court on behalf of the parents of Sam Nelson, a 19-year-old who died from an accidental drug overdose after following dosage advice generated by ChatGPT. The complaint describes how Sam developed a significant reliance on ChatGPT over 18 months. During this period, the product's long-term memory features had archived that he had a major substance abuse and polysubstance abuse problem. Despite this, ChatGPT continued providing specific advice on dosage and substance combinations.

The complaint further alleges that OpenAI and its CEO rushed GPT-4o to market without adequate safety testing, and that over 40 million people consult ChatGPT Health daily. Claims are brought against OpenAI Foundation, OpenAI Holdings LLC, OpenAI Group PBC, and the CEO personally. These include strict product liability for defective design and failure to warn, negligent design and failure to warn, violations of California's unfair competition law, and violations of California business and professions codes prohibiting the unlicensed practice of medicine.

The case raises significant questions about AI product liability, the adequacy of safety testing for consumer-facing AI, and the boundaries of what AI systems may permissibly advise on in health-related contexts.

[18] https://leg.colorado.gov/bills/SB26-051, accessed on May 29,2026.
[19] https://techjusticelaw.org/cases/turner-scott-v-openai-foundation-formerly-openai-inc-openai-holdings-llc-openai-group-pbc-and-samuel-altman/, accessed on May 29,2026.

18	**Multiple Lawsuits filed over AI Voice Training Data** Three separate complaints were filed in the United States District Court for the Northern District of Illinois, Eastern Division, by seven journalists and audiobook narrators, alleging that their voice biometric data was collected and used to train commercial AI systems without notice, consent, or written release, in violation of the Illinois Biometric Information Privacy Act, 2008 (**"BIPA"**). In one complaint[20] the plaintiffs allege that Microsoft Corporation extracted voiceprints from hundreds of thousands of hours of publicly available recordings, including journalism, podcasts, and audiobooks, to build Copilot and Azure voice products. The complaint highlights a telling contradiction: Microsoft Corporation blocks its own opt-in voice enrolment feature entirely in Illinois, treating it as biometric data collection subject to BIPA, yet allegedly applied no equivalent safeguard when extracting voiceprints from publicly sourced recordings. Another alleges[21] that Alphabet Inc. and its subsidiary Google LLC (**"Google"**) scraped long-form, single-speaker, studio-quality recordings that matched their own documented criteria for optimal AI training audio. These voiceprints were used to build foundational voice models powering products including Gemini Live, NotebookLM Audio Overviews, YouTube auto-dubbing, Google Cloud Text-to-Speech, and Google Assistant. The complaint further alleges that Alphabet Inc. and Google had actual knowledge of BIPA, having previously lost hundreds of millions of dollars in BIPA settlements, and had separately built consent-based voice systems for paid voice actors, yet deliberately chose not to extend equivalent protections to creators whose recordings were publicly accessible. A third complaint alleges[22] that NVIDIA Corporation ingested their recordings to build commercial voice products, including tools marketed for studio dubbing and podcast narration, products that now directly compete with the very creators whose voices were used to train them, without providing the written notice, consent, or retention policy BIPA requires. *All three complaints draw a consistent allegation: that each company established formal consent protocols for paid voice actors while deliberately bypassing equivalent requirements for creators whose recordings were publicly accessible, treating public availability as a substitute for consent that BIPA does not recognise.*

[20] Flowers et al v. Microsoft Corporation (No. 1:2026-cv-05491, N.D. Ill.),
[21] Marin et al v. Alphabet, Inc. (No. 1:2026-cv-05436, N.D. Ill.)
[22] Rogers et al v. NVIDIA Corporation (No. 1:2026-cv-05478, N.D. Ill.)

| EUROPEAN UNION

19 **Government agreed to simplify AI Act with expanded prohibitions, including ban on Nudification Apps**[23]

The Parliament along with the Council reached a provisional political agreement on a Digital Omnibus[24] package that amends and simplifies the Artificial Intelligence Act, 2024 **("AI Act")**. As part of the EU's broader competitiveness agenda, the agreement delays the application of rules governing most high-risk AI systems in specified areas, including biometrics, critical infrastructure, education, employment, migration, and asylum, to December 2, 2027, while systems integrated into regulated products such as lifts and toys will be governed by rules effective August 2, 2028. Watermarking and labelling obligations for AI-generated content are brought forward to December 2, 2026.

Alongside simplification, the agreement introduces a significant new prohibition. AI systems that generate sexually explicit images, video, or audio of identifiable persons without their consent, and AI systems that generate child sexual abuse material, will be banned with a compliance deadline of December 2, 2026. Violations carry fines of up to EUR 35 million or 7% of global annual turnover, whichever is higher, representing the highest tier of penalties.

For businesses operating AI systems in any of the high-risk categories listed, the delay to December 2, 2027 provides additional preparation time, but the new prohibitions on non-consensual intimate imagery and child sexual abuse material take effect significantly earlier and require immediate compliance assessment.

[23] https://digital-strategy.ec.europa.eu/en/news/eu-agrees-simplify-ai-rules-boost-innovation-and-ban-nudification-apps-protect-citizens, accessed on May 29,2026.
[24] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718, accessed on May 30,2026.

20 **Privacy Regulator initiated Inquiry into Fashion Platform's Data Transfers to China**[25]

DPC, acting as the lead supervisory authority under the GDPR for entities headquartered in Ireland, opened a formal inquiry into Infinite Styles Services Co. Ltd. (**"SHEIN Ireland")**, the Irish entity of online fashion retailer SHEIN to examine whether transfers of personal data of EU and EEA individuals to China comply with the requirements of the GDPR. The inquiry will assess whether appropriate safeguards were in place for such transfers, as well as compliance with transparency and broader data processing obligations under the GDPR.

The investigation reflects increasing regulatory scrutiny of cross-border data transfers, particularly where personal data is transferred to jurisdictions that do not benefit from an EU adequacy decision. The DPC has identified transfers of personal data to China as a strategic enforcement priority and is expected to coordinate with other European regulators as part of the inquiry.

For businesses with global operations, this investigation serves as a reminder that cross-border data transfers remain one of the most closely scrutinised areas of privacy compliance. Organisations can no longer treat international transfers as a routine operational exercise. Regulators increasingly expect businesses to assess transfer risks, implement appropriate safeguards, and demonstrate that personal data continues to receive an equivalent level of protection after it leaves the EU. As enforcement activity in this area grows, transfer governance is becoming as important as the transfer mechanism itself.

21 **EDPS launched AI Regulatory Sandbox Pilot for EU Institutions**[26]

EDPS launched a pilot AI regulatory sandbox for EU institutions, bodies, offices, and agencies, marking an early and significant step in operationalising the innovation framework under the EU AI Act. The broader AI Act framework requires Member States to ensure at least one national AI regulatory sandbox is operational by August 2, 2026, though this deadline is expected to be extended to August 2, 2027 under the Digital Omnibus proposals published on May 13, 2026.

The sandbox provides a controlled environment for the development, training, testing, and validation of innovative AI systems before deployment, with competent authorities required to provide participants with regulatory guidance and may issue exit reports that can be used to demonstrate compliance through the conformity assessment process.

The EDPS pilot is the first sandbox initiative at the EU institutional level under the AI Act and signals the EDPS's intent to exercise its AI Act authorities actively.

22 **Commission released Draft Guidelines for Transparency Obligations under the AI Act**[27]

The European Commission published *Draft of the guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of the AI Act* **("Guidelines")** with the consultation open until June 3, 2026. Article 50, applicable from August 2, 2026, requires providers of AI systems that interact with individuals to inform those individuals they are interacting with an AI system, and requires providers of generative AI systems to implement machine-readable watermarks enabling detection of AI-generated or manipulated content.

Deployers are separately required to inform individuals when they are exposed to deepfakes, AI-generated publications on matters of public interest, and emotion recognition or biometric categorization systems. The Guidelines, which take into account input from earlier consultations, are

[25] https://www.dataprotection.ie/en/news-media/dpc-opens-inquiry-infinite-styles-services-co-ltd-shein-ireland, accessed on May 29,2026.
[26] https://www.linkedin.com/posts/edps-has-just-launched-a-pilot-project-share-7455525690919284736-BRJb/, accessed on May 29,2026.
[27] https://digital-strategy.ec.europa.eu/en/consultations/consultation-draft-guidelines-transparency-obligations-under-ai-act, accessed on May 29,2026.

being developed in parallel with a voluntary Code of Practice on transparency of AI-generated content and are directed at companies ranging from startups to large enterprises, public authorities, academia, and civil society.

Businesses deploying AI systems that interact with individuals or generate content need to assess watermarking, disclosure, and labelling obligations now, before the guidelines are finalised.

23 **NOYB files complaint against Platform over Paywall on Profile Visitor Data**[28]

The European privacy advocacy organization NOYB-European Centre for Digital Rights **("NOYB")** filed a formal complaint with the Austrian Data Protection Authority against LinkedIn Ireland Unlimited Company (**"LinkedIn"**), alleging violation of the data subject access right under Article 15 of the GDPR. The complaint, registered as NOYB case C104, arises from LinkedIn's practice of restricting profile visitor data including the identities of users who viewed a profile to paying Premium subscribers at approximately EUR 29.74 per month, while simultaneously using privacy and third-party rights as grounds to deny the same data to free users exercising a statutory access request.

Following a data access request submitted in October 2025 via LinkedIn's own download tool, the complainant received no profile visitor data. LinkedIn responded that visitor information belongs to other members and will not be disclosed. NOYB's legal analysis identifies a structural contradiction: as the same data is commercially shared with premium subscribers, LinkedIn's invocation of third-party rights as a shield against free access cannot be legally sustained.

Monetising user data commercially while invoking privacy law to deny access to the same data is a contradiction that regulators will not overlook. Businesses operating tiered data access models should urgently audit whether their access responses are consistent with what they commercially share.

24 **Belgian DPA imposes three fines in separate GDPR Proceedings**[29]

The Disputes Chamber of the Belgian DPA issued three enforcement decisions on May 12, 2026. First, a total fine of EUR 86,000 was imposed on the Société Wallonne des Eaux, a Walloon public water utility, for multiple violations identified during an investigation into contact center call recording practices, including lack of transparency towards callers, absence of a signed data processor agreement for nearly 5 years, unlawfulness of certain test recordings, and retention of call recordings beyond the 1-month limit required to qualify for the contact center exception.

Second, a fine of EUR 120,000 was imposed on Isabel NV/SA, a Belgian fintech company, for misclassifying itself as a data processor rather than a data controller in respect of its TruliUs authentication service, which collected sensitive personal data including national register numbers and identity card photographs, and for the cascade of violations this misclassification caused, including failure to inform users and failure to respond to access requests. Lastly, a fine of approximately EUR 176,000 was imposed on a large technology company for retaining a former employee's corporate mailbox for over a year without lawful basis, failing to inform the employee or her contacts of ongoing processing, and failing to honor her access and erasure requests.

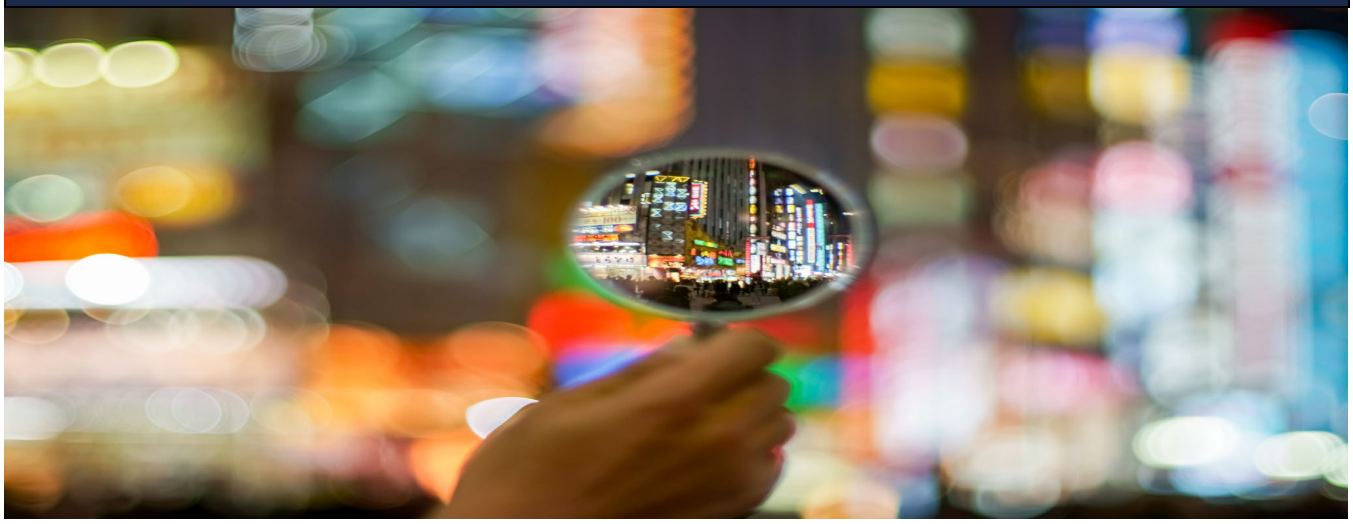
Call recording, processor misclassification, and post-employment data retention are everyday operational realities and precisely what regulators are actively targeting. If your business engages in any of these practices without a clear legal basis and documented compliance framework, the exposure is real and immediate.

[28] https://noyb.eu/en/linkedin-locks-your-gdpr-rights-behind-paywall, accessed on May 29,2026.
[29] https://www.gegevensbeschermingsautoriteit.be/de-geschillenkamer-legt-3-boetes-op, accessed on May 29,2026.

25	**Commission releases Ethical Guidelines on AI and Data in Teaching and Learning** The European Commission, through the European Education Area initiative, released updated *Ethical guidelines on the use of artificial intelligence and data in teaching and learning for educators*[30] ("**Guidelines**"). The Guidelines address the practical and ethical dimensions of integrating AI tools into educational environments, covering core principles including transparency, fairness, the promotion of human agency, and the protection of student data in AI-powered educational tools. The Guidelines specifically address risks arising from AI systems that collect, profile, or process student data at scale, the pedagogical implications of AI-generated content in assessments and coursework, and the duty of educators to model responsible AI use. Complementing the Guidelines, the European Parliament Research Service published a briefing[31] titled *Artificial Intelligence in Classrooms: Pedagogical Dimensions* ("**Briefing**") examining how AI tools affect personalized learning, teacher workload, student engagement, and assessment integrity, and discussing the regulatory interaction between the EU AI Act's high-risk classification for AI systems used in education and the practical realities of classroom deployment. *EdTech businesses and institutions deploying AI tools in educational settings need to assess compliance against both these guidelines and the EU AI Act's high-risk classification for education-sector AI. Student data protection and transparency in AI-generated assessments are now firmly in the regulatory frame.*

[30] https://education.ec.europa.eu/news/ethical-guidelines-on-the-use-of-artificial-intelligence-and-data-in-teaching-and-learning-for-educators, accessed on May 29,2026.
[31] https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/784574/IUST_BRI(2026)784574_EN.pdf, accessed on May 29,2026.

| OTHER COUNTRIES



26	**Japan – Cabinet approved Bill to amend Act on Protection of Personal Information**[32] The Cabinet approved a Bill for Partial Amendment of the Act on the Protection of Personal Information and Other Related Law ("**Bill**") to amend the Act on the Protection of Personal Information ("**APPI**") and submitted it to the Diet for passage. The Bill pursues two objectives: facilitating data utilisation and strengthening enforcement. On utilisation, the amendments introduce a new consent exemption for statistical processing and AI development, enabling organizations to use publicly available sensitive personal data and share personal data with third parties for such purposes, subject to transparency obligations and contractual safeguards. They also introduce a broader exception for processing that does not prejudice individuals' rights and interests, and lower the threshold for existing public-interest exceptions. New specific protections for children's personal data are also introduced, requiring parental consent for children under 16 and granting enhanced rights to request deletion or suspension of data use. On enforcement, the Bill introduces administrative fines for the first time under the APPI, establishing a penalty regime that sits alongside the current framework of directions and criminal sanctions. The fine amount is calculated to confiscate the economic benefit obtained from the violation, with a multiplier for repeat offenders. *If the Bill passes the Diet in 2026, the new rules are expected to take full effect by 2028 at the latest. The introduction of administrative fines marks a structural shift in how data protection obligations are enforced in Japan and raises the stakes of non-compliance considerably.*
27	**China – Government released Policy Framework for Agentic AI**[33] CAC, the National Development and Reform Commission, and the Ministry of Industry and Information Technology jointly issued the *Implementation Opinions on the Standardised Application and Innovative Development of Intelligent Agents* (**"AI Framework"**), marking the first systematic policy framework in which agentic AI, meaning AI systems capable of autonomous, multi-step action and decision-making, is

[32] https://www.ppc.go.jp/news/press/2026/260407/, accessed on May 30,2026.
[33] https://english.www.gov.cn/news/202605/08/content_WS69fde8e2c6d00ca5f9a0ad49.html, accessed on May 29,2026.

treated as a distinct governance category rather than simply an application layer over large language models.

The AI Framework define an intelligent agent as an AI system capable of autonomous perception, memory, decision-making, interaction, and execution, and addresses baseline compliance obligations for developers, providers, and users of such systems. Security assessment requirements, algorithm filing obligations, and risk controls for high-impact systems are among the substantive obligations introduced, alongside sandbox mechanisms to encourage responsible innovation.

China is the first major jurisdiction to treat agentic AI as a distinct regulatory category; others are likely to follow.

28 **China – Court upheld Labour Rights in AI-driven Job Displacement Case**[34]

The Hangzhou Intermediate People's Court ruled in a labour dispute arising from a quality assurance supervisor whose role was taken over by AI large language models, affirming that the employer's dismissal was unlawful and that AI-driven job displacement does not in itself constitute the major change in objective circumstances that can justify contract termination under China's Labor Contract Law.

The employee, Zhou, had joined an AI technology company in November 2022 at a monthly salary of 25,000 yuan, performing tasks including matching user queries with LLMs and filtering illegal or privacy-violating content. When AI systems took over his functions, the company attempted to reassign him to a lower-level position at 15,000 yuan, after he refused, it terminated his contract and offered statutory compensation. The court found that the company's grounds for dismissal did not constitute a major change in objective circumstances, that the company had not demonstrated the contract had become impossible to perform, and that the alternative position offered at a substantially reduced salary was not a reasonable reassignment. The ruling was published by the court as one of a set of typical examples of rights protection at the AI-labour intersection, ahead of International Workers' Day 2026.

Employers using AI to restructure roles cannot simply terminate contracts on the basis that AI has replaced a function. Reasonable reassignment at comparable terms is required and what counts as reasonable is now being tested in court. HR and legal teams need to factor this into any AI-driven workforce restructuring plan.

29 **Malaysia – Court held Bank liable for failing to monitor Customer Accounts**[35]

The Sessions Court in Kuala Lumpur held that Malayan Banking Berhad ("**Maybank**") was liable in negligence for failing to adequately monitor a customer's accounts and detect suspicious transactions that resulted in the unauthorised transfer of RM 166,000. The court allowed the civil claim of Chan Yan Li, who had held two accounts with Maybank since 2000 and discovered in 2021 that RM 166,000 had been transferred from her housing loan account into her savings account and subsequently out to unknown individuals across multiple transactions, with no SMS alerts or push notifications received for the initial transfer.

The court found contradictions between telco records and the transaction reports, noted that several transactions occurred in the early hours of the morning, and held that the sudden and unusual pattern of account activity constituted clear signs of suspicious transactions that should have triggered further verification by the bank. Maybank was ordered to pay RM 166,000 in damages and RM 50,000 in costs. Three individuals linked to mule accounts in the matter had previously pleaded guilty to related offences.

[34] http://english.scio.gov.cn/chinavoices/2026-04/30/content_118471189.html, accessed on May 29,2026.
[35] Chan Yan Li v. Malayan Banking Berhard, Guaman No. WA-A52NCVC-143-02/2022.

Transaction monitoring is not optional, and the absence of real-time alerts for unusual account activity is a negligence risk. If your fraud detection systems cannot flag early-morning, multi-transaction patterns, that gap is a liability.

30 **Argentina – Supreme Court struck down Inter-Agency Data Transfer Provisions**[36]

Supreme Court of Justice of the Nation ("**CSJN**") delivered a ruling with significant implications for the lawfulness of personal data transfers between state agencies. The case arose from a habeas data action by a pensioner seeking to prevent her telephone number and email, provided to the National Social Security Administration ("**ANSES**") for pension management, from being transferred to the Secretariat of Public Communication under Resolution 166E/2016.

The CSJN admitted the appeal and examined the constitutional validity of those provisions. While acknowledging that a literal reading of the provisions permitted the transfer, the court found that their breadth was constitutionally unreasonable. By allowing the consent requirement to be bypassed across a disproportionately wide range of cases, the provisions impinged on the rights to privacy and informational self-determination guaranteed under the Argentine National Constitution. The court confirmed the appellate court's ruling and declared Articles 5(2)(b) and 11(3)(c) of Law 25,326 unconstitutional.

The ruling carries significant implications for how personal data collected by state agencies for a specific purpose may be shared with other government bodies, establishing that the exercise of governmental powers alone is not a sufficient basis to override data subject consent where the transfer falls outside the purpose for which the data was originally collected.

31 **Canada – Privacy Authorities concluded Joint Investigation over AI Platform**[37]

The Office of the Privacy Commissioner of Canada ("**OPC**"), the Commission d'accès à l'information du Québec ("**CAI**"), the Information and Privacy Commissioner for British Columbia ("**OIPC-BC**"), and the Information and Privacy Commissioner of Alberta ("**OIPC-AB**") published their joint findings concluding a multi-year investigation into OpenAI OpCo LLC's privacy practices in relation to the development and deployment of ChatGPT, specifically the GPT-3.5 and GPT-4 models. The Offices found that OpenAI's collection of personal information from publicly accessible websites and licensed datasets for model training was overbroad and did not satisfy the necessity and proportionality requirements under the applicable Acts, and that valid consent was not obtained for this collection.

The findings diverged across jurisdictions on resolution. The OPC found the matters well-founded and conditionally resolved under PIPEDA, taking into account OpenAI's post-investigation implementation of a personal information detection and masking tool, the deprecation of GPT-3.5 and GPT-4, and commitments to enhanced transparency for Canadian audiences including a dedicated blog post explaining its privacy practices. The OIPC-BC and OIPC-AB found the same matters well-founded but unresolved under their respective provincial Acts, as OpenAI's mitigation measures did not satisfy the distinct requirements for implicit or deemed consent under British Columbia's PIPA and Alberta's PIPA.

The divergence in resolution across federal and provincial regulators highlights that compliance with one Canadian privacy framework does not guarantee compliance with others, a consideration of direct relevance to organizations collecting personal data for AI training across multiple Canadian jurisdictions.

[36] Torres Abad, Carmen c/ EN - JGM s/ hábeas data, CAF 49482/2016/CA1-CS1.

[37] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2026/pipeda-2026-002/, accessed on May 29,2026.

ABBREVIATIONS

The following abbreviations are used throughout this newsletter.

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
CAC	Cyberspace Administration of China
DPDP Regulations	Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025
DPC	Data Protection Commission
DPBI	Data Protection Board of India
EEA	European Economic Area
EDPS	European Data Protection Supervisor
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GST	Goods and Services Tax
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
IT Amendment Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026
KYC	Know Your Customer
MeitY	Ministry of Electronics and Information Technology
MoU	Memorandum of Understanding
PIL	Public Interest Litigation
PROGA	Promotion and Regulation of Online Gaming Act, 2025
PIPEDA	Personal Information Protection and Electronic Documents Act
PIPA	Personal Information Protection Act
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
TRAI	Telecom Regulatory Authority of India
UIDAI	Unique Identification Authority of India
UTs	Union Territories

ABOUT THE FIRM

Fountainhead Legal

Technology Law & Data Privacy | General Corporate | Indirect Tax | Living Wills | Litigation Management

Fountainhead Legal is an emerging law firm specialising in data privacy and technology law, with complementary expertise in indirect taxation, general corporate advisory, living wills, and litigation management. 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.

OUR TEAM

Rashmi Deshpande, the founder and partner 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.

FOUNTAINHEAD LEGAL

GET IN TOUCH

CONTACT US

OFFICE

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

CONNECT

Email: rashmi@fountainheadlegal.com / aarushi@fountainheadlegal.com / vaibhav@fountainheadlegal.com

Website: https://fountainheadlegal.com/

LinkedIn: https://www.linkedin.com/company/fountainhead-legal/posts/?feedView=all

NEWSLETTER SUBSCRIPTIONS

To subscribe, unsubscribe, or update your preferences for the Tech & Data Privacy Bulletin, please write to:

[rashmi@fountainheadlegal.com]

DISCLAIMER

This newsletter is prepared by Fountainhead Legal for informational purposes only and does not constitute legal advice or create an attorney-client relationship. Readers should seek specific legal advice before acting on any content herein. The views expressed are those of the authors and do not necessarily represent the official position of the firm.