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 **[JUNE 2026]**

FROM THE DESK OF OUR FOUNDER

FOUNDER'S NOTE

The most important lesson from June is that legal risk is increasingly hidden in ordinary business tools. A tracking pixel installed for advertising or analytics was found to collect sensitive health information without proper consent. A health-related form used for a valid operational purpose still attracted regulatory action because the notice was unclear and the data was kept for too long. These developments should prompt businesses to examine what their websites, applications and forms actually collect, when collection begins, who receives the data and how long it is retained.

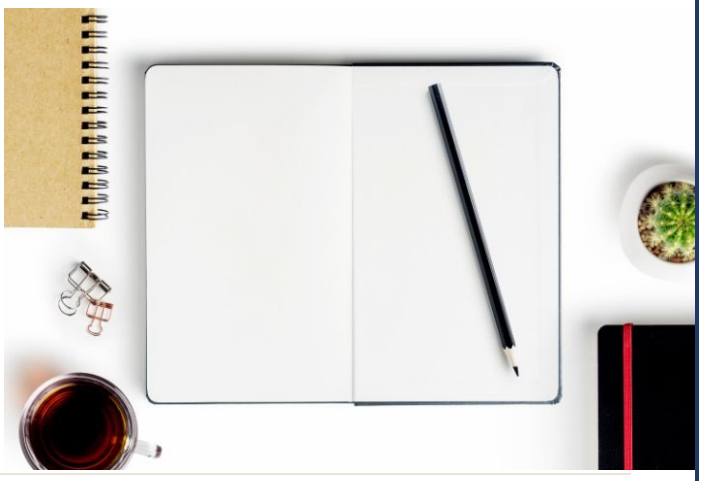
Product and customer journeys also require closer attention. The RBI's action against dark patterns and compulsory bundling makes it clear that customer consent cannot be created through pre-ticked boxes, default selections or confusing sales flows. This approach closely aligns with the DPDP consent framework. Businesses should review the complete journey, from the first screen or sales call to the final agreement, and ensure that product acceptance, marketing permissions and use of personal data are kept clear and separate.

AI is moving from an innovation issue to a governance issue. The RBI's proposed model-risk framework places responsibility on the regulated entity even where an AI model is supplied by a third party. Businesses using AI for credit, fraud detection, customer support, pricing or risk decisions should know which models are in use, what decisions they support and whether their outputs can be explained, tested and reviewed by people.

The platform cases raise wider questions that will also matter to businesses. Courts are considering whether a generative AI service can claim intermediary protection when it creates a fresh response, rather than merely displaying third-party content. The temporary block on an entire messaging application also shows the extent of the Government's powers where a platform is used for organised misconduct affecting public interest.

Other developments in this edition cover the right to be forgotten, access to cloud-stored data after death and the correct preservation of electronic evidence. Each addresses a different issue, but the practical message is clear: businesses must understand how their systems work in practice. Policies remain important, but they will not protect an organisation where the technology, product design or day-to-day process does not follow them.

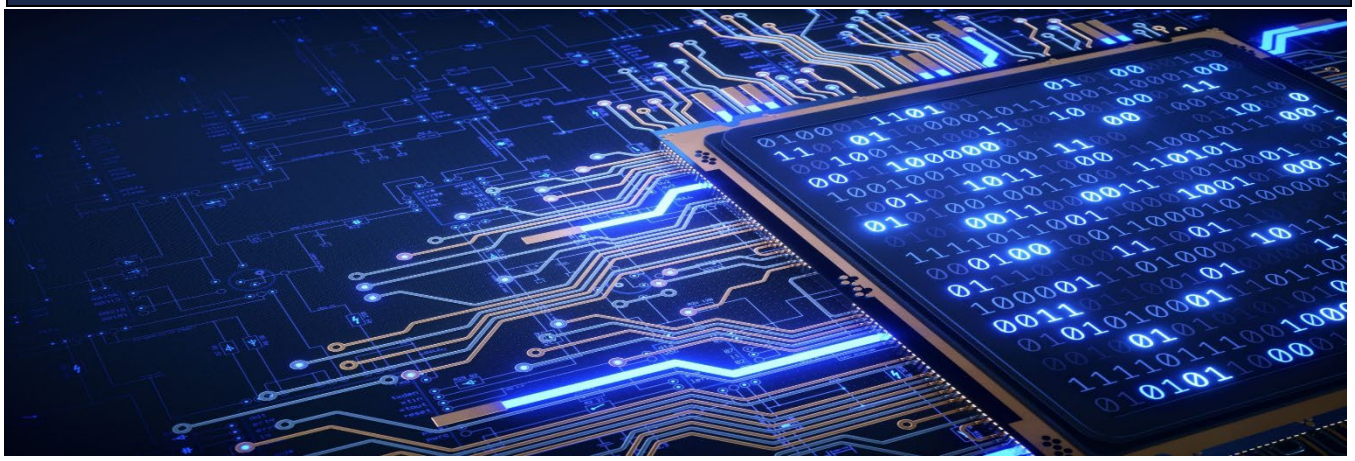
We hope you find this edition insightful!



IN THIS ISSUE

TABLE OF CONTENTS

| INDIA



1 **Delhi High Court recognised Right to be Forgotten in Judicial Records**[1]

The Delhi High Court considered a batch of petitions filed by individuals whose names continued to appear in online judicial records after acquittals, quashed proceedings, settlements, matrimonial disputes and other private matters. The Court held that the right to be forgotten forms part of informational privacy protected under Article 21 of the Constitution. It also clarified that the absence of a specific statute does not prevent constitutional courts from granting appropriate relief where continued online accessibility causes disproportionate harm to a person's privacy, dignity or reputation.

The court drew a careful distinction between preserving a judicial record and allowing that record to remain indefinitely discoverable through a person's name. It explained that de-indexing does not erase a judgment. The record remains available through the case number, citation and other purposeful search terms, while the individual's name is disabled as an unrestricted search key. The court also recognised masking, under which personal identifiers may be replaced with neutral references in publicly accessible versions. Google, Indian Kanoon and the concerned intermediaries were directed to implement the relief granted in the petitions before the court.

The ruling should not be read as creating an automatic right to remove every unfavourable court record. Relief will remain fact-specific and must be balanced against open justice, public interest and freedom of expression. However, search engines, legal databases and platforms hosting public records may now need a clear process to assess and implement de-indexing or masking orders without altering the underlying judicial record.

2 **Consumer Protection Court penalised Edtech Platform for Dark Patterns**[2]

CCPA has imposed penalties imposed a penalty of INR 5 lakh on PhysicsWallah Limited (**"Company"**) for interface practices that interfered with genuine consumer choice. The CCPA found that INR 10 contribution to the PW Foundation was automatically added and pre-selected during checkout, requiring the consumer to notice and remove it. The Company also used messaging connected with children's education and healthcare while presenting the contribution. Separately, users seeking access to content

[1] Laksh Vir Singh Yadav v. Union Of India W.P.(C) 1021/2016
[2] Case No. YY-2/4/2025-CCPA and Case No. YY-2/94/2025-CCPA

advertised as "free" were required to provide personal details such as their mobile number and email address, even though the content offered did not change based on the information collected.

The practices were examined under the *Guidelines for Prevention and Regulation of Dark Patterns, 2023*. Pre-selecting an additional payment was treated as basket sneaking, while attaching unnecessary data collection to a free service raised concerns of forced action. CCPA directed the Company to discontinue the practices and ensure that consumers are able to make an informed and unpressured choice.

The order shows that dark-pattern enforcement is moving beyond misleading advertisements to the design of checkout, consent and data-collection journeys. EdTech, e-commerce, SaaS and subscription businesses should review whether add-ons are pre-selected, whether a refusal option is equally visible and whether personal data is genuinely necessary for a free product or feature. A technically available opt-out may not be sufficient where the interface is designed to steer the consumer towards a particular outcome

3 **Delhi High Court upheld Temporary Nationwide Block on Messaging Application** [3]

MeitY temporarily blocked public access to Telegram across India from June 16 to June 22, 2026, ahead of the NEET-UG re-examination. The Government said organised cheating networks were using Telegram channels to offer purported leaked question papers and mislead candidates. The application was also removed from app stores during the restriction. Telegram argued that misuse by a limited set of users could not justify disabling the service for its wider user base.

Telegram challenged the service-wide restriction before the Delhi High Court and it declined to interfere, holding that the Government was empowered to block public access to Telegram and that the temporary measure was legal and reasonable in the circumstances. The decision is significant because the direction did not merely remove identified channels, accounts or messages; it suspended access to the application itself for users across India. Although the restriction has expired, the ruling demonstrates that the blocking power under Section 69A of the IT Act may extend to an entire computer resource where the Government establishes that narrower measures are inadequate.

The case shows that where a platform is used for organised misconduct affecting significant public interest, the Government may invoke Section 69A to restrict access to the entire application, rather than only specific accounts or content. Such action should remain exceptional, reasoned, proportionate and time-bound. Businesses operating digital platforms should therefore maintain effective misuse controls and rapid response mechanisms, as failure to contain serious misuse may invite service-wide restrictions.

4 **Calcutta High Court dismissed Marketplace Company's Application against AI Company**[4]

The Calcutta High Court delivered its judgment dismissing IndiaMART InterMesh Limited (**"IndiaMART"**) 's application for relief against OpenAI's ChatGPT. IndiaMART, a business-to-business portal operating since 1996, alleged that ChatGPT was deliberately excluding it from responses when users searched for suppliers. ChatGPT bypassed IndiaMART and directed queries straight to seller websites, while working links to rival platforms were provided. IndiaMART contended this amounted to dilution of its trademark, disparagement, and unfair trade practice. It emerged that OpenAI declined to feature IndiaMART content because the platform appears on the United States Trade Representative Notorious Markets List, 2024 - a foreign list that IndiaMART argued carries no statutory force in India.

The court dismissed the application on the foundational ground that there is no legal right to visibility on a private platform. No contract, no statute, and no constitutional provision creates an obligation for a private

[3] Telegram FZ LLC & Anr v. Union of India & Ors, W.P. (C) 8259/2026 & CM APPL. 39036/2026
[4] IndiaMart InterMesh Limited v. Open AI Inc. and Others [IA No. GA-COM/1/2025 in IP-COM/57/2025]

business to promote or feature another on its own service, and without a legally recognised injury there is no actionable cause. On the intellectual property grounds, the court found no falsity, deception, confusion, or publication that would sustain a claim. The court, however, made a significant observation on the more fundamental question: that ChatGPT, which curates, generates, and creates original output rather than merely passing on third-party content, prima facie resembles an originator more than a passive intermediary. However, the opposing view that no output appears without a user prompt also has force. The court held that this vexed question requires expert evidence at a full trial and noted that the IT Act was enacted well before generative AI and may require fresh legislation.

The judgment has significant implications for AI-adjacent litigation in India. The court's observation that generative AI may be an originator, not an intermediary, directly challenges the liability shield that platforms have historically claimed under the safe harbour provisions of the IT Act. Businesses that operate or engage with AI platforms, whether as users, complainants, or developers, should note that this question is now formally live before Indian courts and that legislation may be required to resolve it definitively.

5 **RBI amended Directions on Limiting Customer Liability in Digital Transactions**[5]

RBI issued final *Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026* (**"Amendment Directions"**) revising the framework for customer liability in digital banking transactions, with effect from January 1, 2027. Amendment Directions are no longer limited to transactions carried out without the customer's authorisation. It also covers fraudulent electronic banking transactions induced through deception, coercion or similar fraud, including card-present and card-not-present transactions. A customer will continue to have zero liability where the loss arises from negligence of the bank or a third-party breach, and the bank bears the burden of establishing that the customer is liable.

The Amendment Directions also introduce limited one-time relief for individual customers and sole proprietors who suffer bona fide losses of up to INR 50,000. Subject to the prescribed reporting conditions, the compensation is 85% of the net loss or INR 25,000, whichever is lower. The fraud must be reported to the bank and through the National Cyber Crime Reporting Portal or Helpline 1930 within 5 calendar days. Banks must maintain round-the-clock reporting channels, send transaction alerts and provide provisional credit within the prescribed period for specified transactions while the matter is investigated.

The most important change for banks and payment entities is the shift from relying on standard customer-negligence clauses to proving what occurred in the particular transaction. Institutions will need reliable alert records, fraud-monitoring logs, prompt complaint handling and clear coordination with payment aggregators, gateways and telecom service providers. The January 2027 commencement date should be used to test whether systems can support the evidentiary and response obligations, not only whether policies have been amended.

6 **RBI proposed a Model Risk Framework for AI and Machine Learning**[6]

The RBI has released a draft of *Guidance on Regulatory Principles for Model Risk Management, 2026* ("**Draft Guidelines**") for public consultation till July 26, 2026, setting out for the first time comprehensive and explicit governance expectations for the use of models, including AI and machine learning models, by regulated entities. The Draft Guidelines require a Board-approved model risk management framework covering the complete lifecycle of every model, including selection, development, approval, independent

[5] Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026, RBI/2026-27/167 DOR.MCS.REC.No.130/01-01-032/2026-27

[6] https://rbidocs.rbi.org.in/rdocs/Content/PDFs/DRAFTGUIDANCE24062026FF12A4FF7BC84E8887009D5C5365F8BF.PDF, accessed on June 29,2026.

validation, deployment, monitoring, modification and decommissioning. Models must be classified according to materiality and complexity and maintained in a complete inventory with supporting documentation.

Draft Guidelines expressly covers AI and machine learning models. Regulated entities would be expected to address explainability, bias and fairness, hallucination risk, data drift, overfitting, red-teaming, business continuity and automation bias. Models used for automated decisions must remain subject to meaningful human oversight. Customer-facing generative AI would require additional safeguards and a human alternative. Importantly, the regulated entity remains responsible for the outcome even where the model has been procured from a third-party vendor, and third-party models must also undergo independent validation.

Draft Guidelines treats model risk as an enterprise governance issue rather than a matter left to data science or technology teams. Financial entities using AI for credit, fraud detection, customer service, pricing or risk management should begin identifying every model and the decisions it supports. Vendor procurement will also need stronger due diligence, documentation, access and audit rights, because outsourcing the model will not outsource regulatory accountability.

7 **MHA launched Money Restoration Module for Cybercrime Victims**[7]

MHA launched the *Money Restoration Module* under the National Cyber Crime Reporting Portal to simplify the return of money that has already been traced and frozen in a fraudster's bank account. A victim who has registered the cybercrime complaint and received the acknowledgement number can use the online process instead of repeatedly approaching the police, bank and court for restoration. The mechanism does not create a fresh recovery source; it applies only where the disputed amount has been successfully placed on hold or frozen.

The process distinguishes cases by the amount frozen in each beneficiary account. Where no single account contains more than INR 50,000, restoration may be processed on the basis of the police report and prescribed documentation without a separate court order. Where more than INR 50,000 is frozen in a single account, registration of an FIR is required before the remaining process is completed through the portal. The police upload the necessary documents and the bank credits the approved amount directly to the victim's nominated account.

The module addresses a practical gap between freezing stolen funds and returning them to the victim. Its usefulness will still depend on immediate reporting, since money can be restored only if it is intercepted in time. Banks, FinTechs and consumer-facing digital businesses should therefore make the 1930 Helpline and NCRP reporting process prominent in their fraud-response communications and ensure that internal teams promptly preserve transaction details needed by the police and banks.

8 **RBI prohibited Compulsory Bundling and Dark Patterns in Financial Products**[8]

The RBI issued final amendments to its *Responsible Business Conduct Directions* (**"Directions"**) to curb mis-selling of financial products. Effective January 1, 2027, banks and their agents may not use dark patterns in websites, applications or other sales channels, or make an additional financial product a compulsory condition for obtaining the principal product. Mis-selling includes offering an unsuitable product, giving misleading or incomplete information, selling without explicit consent and bundling products in a manner that removes genuine customer choice.

[7] https://mrm-ncrp.mha.gov.in/public-info, accessed on June 29, 2026.
[8] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/1NOTI1159FE64C67CBFC4483828513EE93480433.PDF, accessed on June 29, 2026.

Consent for each product must be clear, informed and recorded; it cannot be assumed through a pre-ticked box or a default selection. Key features, risks, fees and exit conditions must be disclosed upfront. Regulated entities must periodically audit their interfaces for manipulative design and provide simple mechanisms to decline add-ons and marketing communication. Where mis-selling is established, the bank must cancel the sale and refund the amount collected in accordance with the Directions.

The Directions will require banks, NBFCs, fintech distributors and their agents to review not only their contracts, but also their sales journeys, digital interfaces and consent mechanisms. The approach also aligns with the consent framework under the DPDP Regulations, which requires consent to be free, specific, informed and based on a clear affirmative action. Pre-ticked boxes, default selections and bundled consent for additional products, marketing or cross-selling may therefore raise concerns under both frameworks. Key players should ensure that acceptance of each product and any related use of personal data is obtained separately and without influencing the customer's choice.

9 **Cloud-Stored Data held to form Part of Deceased's Estate**[9]

Court of the 3rd Additional Senior Civil Judge at Gandhinagar held that data stored in a deceased person's iPhone and iCloud account, including photographs, videos, documents and contacts, forms part of the deceased person's digital estate. The court observed that the right to privacy does not prevent legal heirs from lawfully accessing and administering such digital assets after death. Where no nominee has been appointed under the DPDP Regulations, legal heirs may seek access through succession proceedings under the Indian Succession Act, 1925. The court also held that technology platforms may be directed by courts to assist legal representatives in recovering and accessing the digital assets of a deceased user.

The judgment bridges an important gap between the DPDP Regulation and the Indian Succession law, and is the first Indian judicial recognition that digital assets are capable of inheritance and administration through established succession law principles. For businesses offering cloud storage, digital wallets, or data services, the ruling signals that court orders requiring platform assistance in succession-related access can be obtained by legal heirs. The absence of a comprehensive digital estate framework in India and the DPDP Regulations' current silence on posthumous data governance means that this area of law is likely to develop further through litigation in the near term.

10 **Supreme Court clarified Certification Safeguards for Electronic Evidence**[10]

The Supreme Court dismissed a challenge to Section 63(4) of BNS which required electronic records produced as secondary evidence to be accompanied by a certificate containing the record's hash value and certification by a technical expert. The petitioner argued that these requirements imposed an unreasonable burden on litigants, particularly because only a limited number of experts were notified under Section 79A of the IT Act.

The court upheld the requirements, observing that a hash value functioned as a digital fingerprint and helped establish that an electronic record had not been altered after extraction. Expert certification provided an additional safeguard against manipulation, particularly given the growing use of AI and deepfake technologies. The court also clarified that certification was not limited to experts notified under Section 79A. A court could recognise any person with demonstrated expertise in computer science or cyber forensics as a qualified expert.

The ruling clarified the requirements for producing emails, messages, CCTV footage, recordings, system logs and digital documents in court. *Businesses should ensure that electronic records are preserved in a*

[9] Sadhna Shah v. NIL, Civil Miscellaneous Application No. 17/2026, Court of Civil Judge, Gandhinagar
[10] Pune Bar Association v. Union of India, W.P. (C) No. 599/2026

forensically sound manner, hash values are recorded at the time of extraction and a clear chain of custody is maintained.

11 **Draft AI Regulations released for Courts**[11]

The Supreme Court released the *Regulations for Use of Artificial Intelligence in Courts, 2026* ("**Proposed Framework**"), inviting stakeholder feedback until June 20, 2026. The Proposed Framework applies across the Supreme Court, High Courts, subordinate courts, adjudicatory tribunals and statutory commissions. It is built around human primacy, judicial independence, fairness, transparency, accountability, data protection and cybersecurity. AI is permitted only as an assistive tool and must remain subordinate to human judgment.

Permitted uses include case management, scheduling, legal research, document summarisation, translation, transcription, accessibility tools, litigant-assistance chatbots and court analytics. The Proposed Framework absolutely prohibits AI-only judicial outcomes, the use of AI for adjudication or sentencing without human control, bail or recidivism risk scoring, predictive profiling of parties and surveillance of judges, lawyers or litigants. It also proposes an Apex Body at the Supreme Court level, AI Committees and Secretariats at the High Court level, technical and ethical impact assessments, an AI Register, periodic audits and an AI Incident Database.

This draws a clear line between using AI to improve court administration and allowing it to influence the exercise of judicial power. Legal technology providers will need to demonstrate accuracy, security, explainability, auditability and effective human oversight before their tools can be deployed in the court system. The framework is also relevant to law firms and litigants using AI-generated material: verification, confidentiality and disclosure cannot be treated as optional safeguards. Stakeholders with an interest in legal AI are advised to engage during the consultation period, as the final regulations will set the governance baseline for the entire court system.

[11] https://cdnbbsr.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/uploads/2026/06/2026060342.pdf, accessed on June 29, 2026.

| UNITED STATES OF AMERICA

12 **White House issued Executive Order on Promoting Advanced AI Innovation and Cybersecurity**[12]

President Donald Trump signed Executive Order 14409, titled *Promoting Advanced Artificial Intelligence Innovation and Security* ("**EO**"). The EO directs federal agencies to strengthen civilian government systems against AI-enabled cyber threats, expand the use of AI-based defensive tools and establish an AI cybersecurity clearinghouse in coordination with industry and critical-infrastructure operators. The focus is on accelerating vulnerability discovery and remediation while improving information-sharing across government and the private sector.

The EO also requires a classified benchmarking process to identify AI models with advanced cyber capabilities as "covered frontier models". It creates a voluntary framework under which developers may engage with the federal government, provide secure access to such models for up to 30 days before broader release and collaborate on selecting trusted early-access partners. The EO expressly states that this mechanism does not authorise mandatory licensing, pre-clearance or Governmental permission for the development or release of AI models.

EO does not create a general pre-deployment approval regime, but it gives the Federal Government a more direct role in evaluating the cyber capabilities of frontier systems. Developers should track the forthcoming benchmarks and consider the confidentiality, intellectual-property and commercial implications of voluntary early access. Critical-infrastructure operators should also expect closer engagement on the use of AI for both defensive security and emerging threat response.

13 **Florida sued Major AI Company Over Safety Concerns**[13]

Florida became the first state in the United States to file a lawsuit against OpenAI Inc. ("**OpenAI**" or **"Company"**) and its Chief Executive Office (**"CEO"**), over the alleged safety failures of the ChatGPT platform. The complaint alleges that the product was made widely available despite known safety risks and that the Company's public statements did not adequately disclose those risks. It raises specific

[12] https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/, accessed on June 29, 2026.
[13] https://www.myfloridalegal.com/sites/default/files/openai-filed-stamped-complaint.pdf, accessed on June 29, 2026.

concerns about protections for minors, collection of children's data, behavioural dependence, self-harm and the use of the system for health-related guidance.

The State relied principally on the Florida Deceptive and Unfair Trade Practices Act, 1973 and sought civil penalties, injunctive relief, restitution and other remedies. The complaint also names Company's CEO personally on the basis of his alleged involvement in the decisions challenged. These are allegations at the pleading stage. They have not been proved, and the Company disputes the State's characterisation of its safeguards and conduct.

The case is significant because it attempts to apply established consumer-protection principles directly to the safety design and marketing of a general-purpose AI product. AI providers should expect regulators to examine whether public claims are supported by internal testing, whether known risks are escalated and whether age controls and crisis-response measures work in practice. Careful documentation of safety decisions may be as important as the safeguards themselves when a product is challenged.

| EUROPEAN UNION

15 **CJEU clarified Platform Liability and Cross-Border Age-Verification Rules**[14]

The ruling arose from challenges to French measures affecting services offered from other EU Member States. Adult-content platforms questioned France's power to require age verification for users in France, while a driving-assistance service challenged restrictions on the sharing of alerts concerning certain roadside checks. The disputes led the French court to seek guidance on the extent to which national rules may apply to cross-border digital services and whether a platform remains a passive host when it controls how user information is displayed.

The CJEU held that a Member State may impose proportionate measures for the protection of minors, public order and public safety, subject to the conditions under EU law. It also indicated that a platform may lose hosting liability protection where its algorithm plays an active role in deciding whether, how and in what order user content is presented. The ruling is important for digital platforms because both the design of their content-ranking systems and the countries in which their services are available may affect their legal obligations.

16 **Italian DPA fined International Airline for Personal Data related Transparency and Retention Failures**[15]

The Italian DPA fined Emirates (**"Company"**) €180,000 following a complaint concerning the medical information form used for passengers requiring assistance or assessment of fitness to travel. The Authority accepted that an airline may process relevant health information without consent where this is necessary to ensure safe transport and provide assistance under applicable sectoral law. The infringement did not arise simply because health data was collected.

The Authority instead found that the Company had not provided sufficiently clear and complete information on who was required to complete the form, which sections were mandatory and how the

[14] Cases C-188/24 and C-190/24

[15] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10261301 , accessed on July 16, 2026.

information would be used. It also considered the seven-year retention period for the medical form excessive in relation to the purpose of organising and completing the journey. The Company was directed to revise its privacy information, define proportionate retention periods and erase data retained beyond the justified period.

The decision is a useful reminder that a valid legal basis does not resolve every compliance question. Organisations using standard forms for health or other sensitive data must separately establish necessity for each field, explain the process at the point of collection and set a retention period tied to the actual purpose. Long retention based on a general corporate schedule is difficult to defend where the operational need is short-lived.

17 **European Commission published AI-generated Content Labelling Code**[16]

The European Commission published *Code of Practice on Marking and Labelling of AI-generated Content* (**"Code"**). The Code provides practical measures to support compliance with the transparency obligations under the EU AI Act, 2024 (**"AI Act"**) that apply from August 2, 2026. It addresses how providers and deployers may inform users that they are interacting with an AI system and how AI-generated or AI-manipulated content can be marked in a consistent and understandable manner.

The statutory obligations cover key situations such as deepfakes, AI-generated or manipulated text published on matters of public interest and interactions with systems such as chatbots. The Code also supports the use of machine-readable methods that enable generated content to be detected. Participation is voluntary, but adherence may help demonstrate the steps taken to meet the AI Act's transparency requirements.

Providers and businesses deploying generative AI in the European Union should treat August 2, 2026 as an implementation date, not the beginning of a planning exercise. User notices, content labels, technical markers and internal responsibility for deciding when disclosure is required should already be built into the product workflow. A generic statement in terms of use will not replace a clear disclosure at the point where the user encounters the AI system or generated content.

18 **Munich Court held Major Search Engine Provider responsible for False Statements in AI-Generated Summaries**[17]

The Regional Court of Munich held, at first instance, that Google could be directly responsible for inaccurate statements generated in its AI Overviews. The dispute concerned statements presented in an AI-generated search summary rather than a conventional list of links to third-party webpages. The Court treated the generated summary as substantive content produced and prominently presented by Google, not merely as neutral transmission or hosting of another person's material.

This distinction was central to the outcome. Liability protections developed for platforms that store or display third-party content do not necessarily apply in the same way where the platform synthesises sources and produces a new answer in its own interface. Google has indicated that it intends to appeal, and the ruling remains a first-instance German decision rather than a Europe-wide determination.

The judgment should not be read as establishing automatic liability for every inaccurate AI response. It does, however, show that courts may focus on who generated and presented the final statement rather than only on the underlying sources. Search and chatbot providers should strengthen source controls, verification, correction and complaint mechanisms, especially where summaries make factual claims about identifiable persons or businesses.

[16] https://digital-strategy.ec.europa.eu/en/news/commission-publishes-code-practice-marking-and-labelling-ai-generated-content , accessed on July 16, 2026

[17] LG München I, Endurteil v. 28.05.2026 – 26 O 869/26

| OTHER COUNTRIES

19	**United Kingdom – Government proposed Social Media Ban for Children under 16 years** Government announced plans to prevent social media platforms from offering their services to users under the age of 16. The proposal is expected to be placed before Parliament before the end of 2026, with implementation targeted for spring 2027. It would cover user-to-user services such as TikTok, Snapchat, YouTube, Instagram, Facebook and X, but is not intended to include messaging services such as WhatsApp and Signal. Government also plans wider online safety rules for children. Children under 16 may be restricted from livestreaming or communicating with strangers on services such as gaming platforms, while similar safeguards may be enabled by default for users aged 16 and 17. AI features designed for intimate or romantic interaction may also be age-restricted. Strong age-verification measures are expected, although the final requirements are yet to be decided. *This is an announced policy rather than an operative ban, and the detailed legislation may change. Social media, gaming and AI providers should nevertheless assess whether their current age-assurance methods, default settings and feature controls could support the proposed model. The main compliance challenge will be to verify age effectively without collecting more identity data than is necessary or creating new privacy and security risks for children.*

20	**United Kingdom – DUA's requirement for establishing Grievance Mechanism enforced**[18] New requirements under DUA came into force on June 19, 2026, requiring organisations to establish a clear process for handling data protection complaints. Organisations must give individuals an accessible way to complain, acknowledge a complaint within 30 days, take appropriate steps to investigate it without undue delay, keep the complainant informed and communicate the outcome.

[18] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/05/one-month-to-go-what-businesses-need-to-know-to-meet-new-data-law/ , accessed on July 16, 2026.

A complaint does not need to cite the UK GDPR or use legal language. It may arise through an ordinary customer-service message, email, call or other channel if the substance concerns the collection, use, disclosure or retention of personal data. The Information Commissioner's Office has published guidance explaining the steps organisations must, should and could take and has emphasised early resolution before a matter escalates to the regulator.

The change turns privacy complaints into a defined operational process rather than a matter handled informally by legal or customer-service teams. Organisations should identify all intake channels, train staff to recognise a data protection complaint, assign ownership, maintain an auditable record and connect the process with data subject rights, breach response and regulatory escalation. International businesses serving individuals in the United Kingdom should ensure that their global complaint procedure can meet the specific UK timelines

21 **Australia – Privacy Regulator ruled against Unauthorised Collection of Health Data through Tracking Pixels**[19]

OAIC issued two determinations concerning Medmate, a telehealth provider, and Monash IVF, a fertility-services provider. It found that third-party tracking pixels on their websites collected sensitive health information without the required consent. The information transmitted through the pixels could reveal matters such as the type of consultation sought, medicines selected or fertility-related actions taken and was used in connection with targeted advertising.

It was held that the website provider remains responsible for the collection caused by the pixel, even where an advertising agency or technology platform is involved. The determinations also reinforce that information may be personal where it allows a person to be singled out, even if a name or conventional identifier is not included. The OAIC published a companion report based on its inspection of 50 health-service websites and urged organisations to review their use of tracking technologies.

The findings are relevant beyond healthcare. Hashed, pseudonymous or event-level data is not automatically anonymous where it can distinguish a user or reveal sensitive activity. Organisations should know exactly what each pixel sends, who receives it and whether it activates before consent. Responsibility cannot be shifted to the advertising vendor through contract alone; the website operator must configure and govern the technology lawfully.

[19] https://www.oaic.gov.au/news/media-centre/privacy-commissioner-finds-privacy-breaches-in-third-party-tracking-pixel-investigation , accessed on July 16, 2026.

ABBREVIATIONS

The following abbreviations are used throughout the June 2026 edition of this newsletter.

ABBREVIATION	FULL FORM
BNS	Bharatiya Nyaya Sanhita, 2023
CCPA	Central Consumer Protection Authority
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DPDP Regulations	Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025
DUA	Data (Use and Access) Act, 2025
IT Act	Information Technology Act, 2000
MeitY	Ministry of Electronics and Information Technology
MHA	Ministry of Home Affairs
OAIC	Office of the Australian Information Commissioner
RBI	Reserve Bank of India

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 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.