Fountainhead Legal

Technology Law | Data Privacy | Regulatory Strategy

FL FOUNTAINHEAD LEGAL

FEBRUARY NEWSLETTER

Where Regulation Meets Enforcement

February 2026

FOUNDERS NOTE

FOUNTAINHEAD LEGAL

This edition brings together a set of developments that showcase how digital regulation is increasingly moving from policy discussions to practical implementation. In India, the Supreme Court examines the interplay between the DPDP Act and the Right to Information framework highlights the continuing effort to balance privacy with transparency. At the same time, the Reserve Bank of India's proposed Responsible Business Conduct Directions for banks and NBFCs point to a stronger emphasis on responsible lending practices, clearer consent mechanisms, and greater accountability in digital financial services. The Government has also introduced amendments requiring mandatory labelling of synthetically generated or AI-manipulated content, reflecting growing regulatory attention to the risks posed by deepfakes and misleading digital media. Complementing these developments, the Government also issued a cybersecurity framework for India's space ecosystem, underscoring the importance of securing satellite communication infrastructure as the country's commercial and strategic space activities expand.

Globally, regulators are focusing more closely on how compliance works in practice. Recent enforcement activity in the United States involving a leading digital media platform demonstrates that privacy rights must operate consistently across platforms and device, while developments in Europe from cybersecurity vulnerabilities affecting regulators themselves to rulings on employee data access, reinforce that accountability ultimately follows control over data. Alongside these regulatory updates, this edition also includes a brief glimpse into some of our firm's recent activities and engagements across our practice areas. We hope you find this edition insightful.

REGULATORY WATCH

INDIA

Government introduces Mandatory Labelling for AI-Generated Content for Intermediaries[1]

MeitY has introduced new compliance obligations for digital platforms through the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026* ("Amendment Rules"). The amendment requires intermediaries to ensure that synthetically generated information including AI-generated or AI-altered audio, visual, or audio-visual content that may influence perceptions of authenticity is clearly labelled.

Intermediaries and Significant Social Media Intermediaries facilitating such content must implement reasonable technical measures, including automated tools, declaration and verification mechanisms, and safeguards to prevent unlawful synthetic content, while also complying with authorised takedown directions within three hours.

These changes are likely to require platforms to strengthen content governance and monitoring mechanisms for AI-generated media. For a brief overview of the amendments and what they mean for platform compliance, please refer to our alert **here**.

Supreme Court refers DPDP-RTI Conflict to Constitution Bench[2]

The Supreme Court issued notice in three writ petitions challenging the constitutional validity of the DPDP Act 2023, and referred the core questions to a five-judge Constitution Bench for hearing on 23 March 2026.

---

[1] https://www.meity.gov.in/documents/act-and-policies/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-it-rules-2021-IjM5QjMtQWa?pageTitle=Information-Technology-(Intermediary-Guidelines-and-Digital-Media-Ethics-Code)-Rules,-2021-(IT-Rules,-2021)

[2] The Reporters Collective Trust v. Union of India (W.P.(C) 211/2026)

At the centre of the dispute is a change introduced through the DPDP framework that affects how personal data held by public authorities may be disclosed under the Right to Information Act, 2005. Petitioners argue that the amendment removes the earlier ability to disclose personal information where a larger public interest justified the disclosure, potentially enabling public authorities to deny such requests even when transparency considerations are involved. The Court declined to stay the operation of the DPDP framework for now, leaving the constitutional question to be examined by the Constitution Bench.

RBI released Draft Code of Conduct Directions for Banks and NBFCs[3]

The Reserve Bank of India has released *Draft Reserve Bank of India (Non-Banking Financial Companies - Responsible Business Conduct) Amendment Directions, 2026 ("Draft Directions")*, open for public consultation until early March 2026, with a proposed effective date of 1 July 2026. The Draft Directions consolidate various conduct-related requirements relating to marketing practices, customer suitability, recovery conduct, and grievance mechanisms into a more structured regulatory framework for banks and NBFCs. Certain categories such as Core Investment Companies and NBFC-Account Aggregators are excluded.

Explicit consent must be a clear, separate action which must be fully documented and not mixed with other terms. Product suitability checks must be recorded. Recovery agent behavior is now a key board-level compliance duty, not just a minor back-office task.

For NBFCs running digital lending apps, embedded finance models, or third-party distribution channels, the consultation window is the last point at which compliance architecture can be shaped rather than inherited.

Government released Cybersecurity Framework for Space Sector[4]

CERT-In has released a Cybersecurity Framework and Guidelines for Space Systems ("Guidelines") aimed at strengthening the security posture of India's growing satellite and

[3] https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=62207
[4] https://www.cert-in.org.in/PDF/CyberSecurityFrameworkGuideline_for_space.pdf

space communications ecosystem. Developed in collaboration with the SatCom Industry Association, the Guidelines addresses cybersecurity risks across key components of the space ecosystem, including satellites, ground stations, communication networks, and user terminals. It identifies threats such as signal jamming, spoofing, unauthorised command access, and compromise of ground infrastructure that could disrupt critical communications and navigation services.

The Guidelines sets out recommended governance structures, risk management practices, and operational safeguards for entities operating in the space sector. It encourages organisations to adopt security-by-design principles, conduct periodic risk assessments, implement robust monitoring and incident response mechanisms, and align incident reporting with CERT-In's existing cybersecurity reporting processes. As commercial space activities expand in India, the Guidelines reflect a growing policy focus on ensuring that space infrastructure much like other critical digital systems incorporates strong cybersecurity controls throughout its operational lifecycle.

USA

California issues Largest CCPA Fine to Date Against a Major Streaming Platform[5]

California Attorney General secured a USD 2.75 million settlement under the California Consumer Privacy Act (CCPA) with The Walt Disney Company ("Company"), marking the largest enforcement action under the law so far. The investigation found that the Company's streaming platforms did not properly honour user opt-out requests for the sale or sharing of personal data. While users could opt out on a specific service or device, the preference was not applied consistently across other services or devices linked to the same account. In addition, some opt-out mechanisms applied only to the Company's own advertising systems while third-party tracking technologies remained active, and Global Privacy Control signals were not fully recognised.

The regulator emphasised that where companies combine consumer data across multiple services for advertising or analytics, they must also ensure that privacy choices apply

[5] https://oag.ca.gov/news/press-releases/california-wont-let-it-go-attorney-general-bonta-announces-275-million

consistently across those services. The decision highlights the growing regulatory focus on how privacy rights operate in practice, particularly for digital platforms that manage user identities across multiple devices and services.

For Indian companies operating digital consumer products with US audiences, this enforcement trajectory establishes the standard against which cross-platform opt-out design will now be assessed. The technical complexity of implementation is not a compliance defence.

NETHERLANDS

Dutch Data Protection Authority's Own Employee Data Compromised in Ivanti Zero-Day Attack[6]

In early February 2026, the Dutch Data Protection Authority ("DPA") which is the country's primary privacy enforcement body, reported that employee data including names, official email addresses and phone numbers had been accessed by unauthorised parties following zero-day vulnerabilities in Ivanti Inc.'s Endpoint Manager Mobile software (CVE-2026-1281 and CVE-2026-1340, both rated 9.8 severity).

The Council for the Judiciary was simultaneously affected. The DPA reported the breach against itself, in an exercise of the same obligations it routinely enforces against others. The incident underscores an accountability question that most compliance programmes underweight: the 72-hour notification obligation and baseline security controls under GDPR apply regardless of the sophistication of the victim organisation. Regulators are not exempt. Vendor software vulnerabilities in widely deployed enterprise tools are, for the purposes of Article 32, your risk to manage, not your vendor's.

NORWAY

Time-Tracking Company Fined for Withholding Employee Data After Employer's Bankruptcy[7]

[6] https://www.enisa.europa.eu/news/joint-statement-on-ivanti
[7] https://www.datatilsynet.no/contentassets/fd51778709a14285a13d4cca9fc481f6/20206-01-16-vedtak---timegrip-offentlig-versjon.pdf

The Norwegian Data Protection Authority fined Timegrip AS EUR 25,000 for refusing access requests from 80 former employees seeking their time records after their employer, a retail chain, declared bankruptcy in 2020.

Timegrip argued that the data processing agreement ended with the bankruptcy and that no controller existed to authorise disclosure. The authority rejected this when Timegrip became the sole entity holding and controlling access to the data, determining who could access it, setting retention periods, handling requests. It was functioning as a controller, not a processor. The processor-controller boundary shifts when a controller ceases to operate. This is the regulatory reality for any human resource technology, Software-as-a-Service payroll, or data processing vendor whose client base includes companies at financial risk. The data subject right does not dissolve because the contractual chain does.

EVENTS ATTENDED

FOUNTAINHEAD LEGAL

On 21 February 2026, our Partner, Rashmi Deshpande, was part of a structured discussion hosted by Gen S Life and EasyInherit examining the legal architecture of advance medical directives including enforceability, documentation standards, and institutional preparedness.

Living wills continue to sit at a complex intersection of constitutional rights, medical ethics, and procedural compliance under evolving Supreme Court jurisprudence. The session focused on clarity over advocacy and on the practical dimensions of implementation.

For those who could not attend, the full discussion is now available here.

Our Partner, Rashmi Deshpande had the opportunity to share a few reflections on what young lawyers often overlook, at the Law Network Forum hosted by MIT World Peace University and CIAP.

The conversation wasn't just about employability - it was about building judgment. That takes time, context, and deliberate training. She discussed about understanding facts before law and learning to write before interpreting law.

MEDIA APPEARANCES

FOUNTAINHEAD LEGAL

Our partner, Rashmi Deshpande, commented to The Indian Express that there is a privacy angle to consider and the requirement to embed permanent metadata and unique identifiers improves traceability and can deter impersonation, fake political content, or non-consensual imagery.

Her comments were carried in the story on India's new 3-hour deepfake removal rule: Experts urge strict compliance where she also pointed out that in situations like the Grok episode, where AI-generated responses created global controversy, the new AI Rules would make platforms more accountable. They cannot simply react after something goes viral, they are expected to prevent harmful or misleading synthetic content from being generated in the first place.

Read the article here.

ABOUT FOUNTAINHEAD LEGAL

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

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

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

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

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

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

FL FOUNTAINHEAD LEGAL

CONTACT DETAILS

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

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

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

Address
C - 2106, Oberoi Garden Estate, Chandivali Farm Road, Powai – 400 072
Website: https://fountainheadlegal.com/
LinkedIn: https://www.linkedin.com/company/fountainhead-legal/