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 **[AUGUST 2026]**

FROM THE DESK OF OUR FOUNDER

FOUNDER'S NOTE

August offered a useful reminder that technology regulation is becoming less about announcing frameworks and more about testing whether organisations are actually prepared to operate within them. The clearest example is the DPDP Act. The Government's push for time-bound implementation across Ministries, States and Union Territories, together with the indication that the notified compliance timeline is not expected to be extended, changes the practical conversation around readiness. The remaining transition period is no longer just a planning window. Organisations now need to close the difficult implementation gaps such as legacy data, consent journeys, retention, vendor arrangements, grievance handling and breach response before the deadline arrives.

SEBI's recent measures point in a similar direction, but through technology resilience. The new IT Resilience Index for market infrastructure institutions seeks to measure how critical systems perform, while the revised cyber incident reporting framework requires incidents to be tracked more systematically as they evolve. This is important because resilience is increasingly being judged through evidence: how quickly an issue was detected, how systems responded, what was recorded and how normal operations were restored.

Semicon 2.0 brings a different dimension to the same discussion. India's digital ambitions depend not only on software, AI and data, but on the physical infrastructure that supports them. By promoting domestic capability in chip design, fabrication, packaging, equipment and research, the Scheme places semiconductor capacity at the centre of the country's technology strategy. For businesses, this can influence decisions around sourcing, product architecture, localisation, intellectual property and long-term technology partnerships.

The DABUS copyright development raises a far more specific, but equally interesting, question: who is the author when an AI system generates the work? The Copyright Office declined to recognise the AI system itself as an author under the Copyright Act, 1957, leaving any such change to Parliament. For businesses already using generative AI to create code, designs, marketing material and other commercial content, the issue is practical. If ownership is later challenged, organisations may need to show who directed the process, what human contribution existed and how the final work was created.

Outside India, the focus is becoming equally granular. The EU AI Act has moved further into application, while the General-Purpose AI Code of Practice gives providers a more workable route for dealing with documentation, copyright, safety and systemic-risk obligations. Digital platform regulation is also moving deeper into recommender systems, interface choices, age-assurance tools and generative AI features. In the United States, ongoing litigation concerning younger users is putting engagement design and children's data practices under judicial scrutiny. China's proposed cyberviolence framework similarly places greater responsibility on platforms to identify abuse, preserve evidence and protect personal information that may be misused.

What stands out this month is how often the legal issue arises before the final product reaches the user. It can begin with how data is collected, how a system is designed, how a model is documented, how a chip is sourced, or how an algorithm shapes user behaviour.

That makes one question especially useful for businesses, where in the technology lifecycle is the legal risk actually being created and is it being addressed at that stage?

We hope you find this edition insightful!

IN THIS ISSUE

TABLE OF CONTENTS

| INDIA

1 **Government notified Semicon 2.0 Scheme for Chip Ecosystem**[1]

Central Government notified the Semicon 2.0 Scheme (**"Scheme"**), with an outlay of INR 1,27,500 crore to support semiconductor design, manufacturing and related capabilities in India. The Scheme covers six areas, including chip design, fabrication, semiconductor equipment and materials, assembly and testing, research and development, and talent development. Eligible participants may access different forms of fiscal support, including seed funding and deployment-linked incentives for chip-design businesses, and capital support for fabrication and advanced packaging facilities.

The Scheme is relevant well beyond semiconductor manufacturing. Chips form the underlying infrastructure for AI systems, data centres, telecom networks, connected devices, automobiles, cloud infrastructure and consumer electronics. By supporting domestic design, fabrication, packaging and related supply chains, Semicon 2.0 seeks to reduce dependence on imported semiconductor capacity while creating greater domestic capability around technologies that increasingly power India's digital economy.

For technology, electronics and hardware businesses, the Scheme may influence decisions around product design, sourcing, localisation and technology partnerships in India. Companies developing AI hardware, connected products or other semiconductor-dependent technologies should assess whether planned investments, intellectual property structures and manufacturing arrangements can be aligned with the incentives available under the Scheme.

2 **SEBI introduced IT Resilience Index and revised Cyber Incident Reporting Framework**

SEBI issued the Circular on IT Resilience Index for Market Infrastructure Institutions (**"ITRI Circular"**) [2] and the Circular on Alignment of SEBI's Cyber Incident Reporting Portal with

[1] https://cdsco.gov.in/opencms/resources/UploadCDSCOWeb/2018/UploadPublic_NoticesFiles/Guidance%20document%20on%20Medical%20Device%20Software%20under%20MDR-2017.pdf, last accessed on August 28, 2026

[2] https://www.sebi.gov.in/legal/circulars/aug-2026/alignment-of-sebi-s-cyber-incident-reporting-portal-with-fire-format_103915.html, last accessed on August 31, 2026

FIRE Format (**"FIRE Circular"**)[3]. Together, the measures strengthen oversight of technology resilience and cyber incident management across the securities market.

Under the ITRI Circular, stock exchanges, clearing corporations and depositories will be assessed against defined resilience parameters relating to system availability, security, governance, continuity and monitoring. The framework also places emphasis on automated measurement and early identification of technology issues. Separately, the FIRE Circular aligns SEBI's reporting process with the Financial Stability Board's Format for Incident Reporting Exchange (**"FIRE"**), so that information relating to a cyber incident can be captured and updated in a more structured manner as the incident progresses.

The two measures are significant because they require regulated entities to demonstrate technology resilience through evidence and reporting, rather than relying only on internal policies. MIIs should be able to show how critical systems are monitored and restored, while other regulated entities should ensure that cyber incidents are consistently recorded, escalated and updated from detection through closure.

3 **Copyright Office held AI cannot be recognised as an Author[4]**

The Copyright office considered an application for registration of an artwork created using DABUS, an artificial intelligence system. The application identified 'DABUS' as the author and Dr Stephen Thaler as the owner of the work. While examining the application under the Copyright Act, 1957, the Copyright office took the view that an AI system cannot itself be recognised as an author under the present statutory framework. For computer-generated works, authorship must ultimately be attributed to a legally recognised person responsible for causing the work to be created.

The application was refused because DABUS continued to be named as the author despite an opportunity to amend the filing. Copyright office also indicated that extending legal authorship to autonomous AI systems would require Parliament to change the law, rather than the Copyright Office expanding the meaning of "author" through interpretation.

The decision is important for businesses increasingly using generative AI to create designs, marketing material, software and other content. The key issue is not simply whether an AI-assisted output can attract copyright protection, but whether the business can identify and document the human involvement behind its creation. Clear internal records of who directed, selected or developed AI-generated content may therefore become important when establishing ownership and enforcing rights.

[3] https://www.sebi.gov.in/legal/circulars/aug-2026/it-resilience-index-for-market-infrastructure-institutions-miis-_103913.html, last accessed on August 31, 2026

[4] Stephen Thaler v. Union of India, W.P.(C)-IPD 15/2026

4 **Parliament passed Bankers' Books Evidence Bill**[5]

Parliament passed the *Bankers' Books Evidence Bill, 2026,* which subsequently received Presidential assent and became the *Bankers' Books Evidence Act, 2026* (**"BBEA"**). BBEA replaces the Bankers' Books Evidence Act, 1891 and updates the manner in which banking records may be produced before courts and other authorities, reflecting the shift from physical ledgers to electronically maintained records.

BBEA recognises bank records maintained in electronic form, including records stored through digital systems and cloud infrastructure, subject to prescribed certification requirements. Banks relying on such records will need to demonstrate the reliability of the relevant systems, the integrity of the data and the absence of unauthorised alteration. The framework also reduces the need for routine production of original physical books and personal appearance of bank officers in proceedings where the bank is not itself a party.

This legislation is significant from a technology and data-governance perspective because the evidentiary value of a bank's records will increasingly depend on the reliability of the systems through which those records are created, stored and retrieved. Banks should therefore ensure that audit trails, access controls, logging, data-retention practices and cloud arrangements are capable of supporting the certifications required when digital records are produced in legal proceedings.

5 **Cyber Security Regulations for Power Sector notified** [6]

The Central Electricity Authority notified the *Central Electricity Authority (Cyber Security in Power Sector) Regulations, 2026* (**"Cyber Security Regulations"**) under the Electricity Act, 2003. The Cyber Security Regulations create a binding cybersecurity framework for entities across the power sector, covering both operational technology used for grid and power infrastructure and the information technology systems connected to business operations.

Covered entities are required to establish dedicated cybersecurity governance, including a 24x7 information security function and designated security leadership. The Cyber Security Regulations also places emphasis on segregation between operational and corporate networks, timely reporting of cybersecurity incidents, restrictions around remote access and localisation of specified operational and telemetry data within India.

The Cyber Security Regulations recognise that cyber risk in the power sector can directly affect physical infrastructure and continuity of essential services. Power-sector entities should therefore review IT–OT connectivity, third-party access, incident-response processes, data-hosting arrangements and vendor controls to ensure that cybersecurity requirements are embedded into day-to-day infrastructure management rather than addressed only through general IT policies.

[5] https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/as intro832026124359PM.pdf?source=legislation, last accessed on August 28, 2026

[6] https://cea.nic.in/wp-content/uploads/notification/2026/08/Cyber_Regulations_Notification.pdf, last accessed on August 28, 2026

6 **Parliamentary Committee called for Faster Progress on Digital Competition Regulation** [7]

Standing Committee on Finance (**"Committee"**) presented *Action taken by the Government on the Observations/Recommendations contained in the Twenty-Fifth Report on 'Evolving Role of Competition Commission of India in the Economy, particularly the Digital Landscape* (**"Report"**) reviewing the Government's progress on competition issues in digital markets. The Report reiterated support for a forward-looking regulatory framework for large digital platforms and urged the Government to advance the Draft Digital Competition Bill, 2024 (**"Draft Bill**"), alongside the existing Competition Act, 2002.

The Committee also highlighted the need to strengthen the CCI's technical capabilities, including expertise in areas such as artificial intelligence and data science, and to improve coordination where competition, platform conduct and data-related concerns overlap. The areas flagged for closer attention include self-preferencing, bundling of digital services, algorithmic decision-making and the use of data by large platforms in ways that may affect market access for competitors.

This review highlights increasing regulatory momentum toward proactive, structural market rules rather than relying solely on lengthy investigations after-market harm occurs. Dominant tech platforms must prepare for heightened scrutiny over how they rank search results, bundle proprietary digital services, and leverage consumer data to prevent rival technology services from competing on an even playing field.

7 **Delhi High Court granted stay against Streaming Websites** [8]

The Delhi High Court considered a suit concerning 30 websites that were allegedly making copyrighted films and other video content available for streaming without permission. Since such websites can quickly reappear through mirror domains, redirects or slightly altered web addresses, the copyright owners sought an order that would cover not only the identified websites but also future variants used to continue the same activity.

Crucially, court granted interim relief against the identified websites. For subsequently discovered mirror or redirect sites, however, it required a controlled process rather than allowing intermediaries to make a final infringement determination on their own. Rights holders may flag such websites and provide supporting material, but the extension of the blocking order must ultimately remain subject to the court's supervision.

The decision is relevant for digital media and streaming businesses because it recognises the speed at which piracy networks can migrate across domains, while preserving a judicial check on website blocking. It therefore supports more effective anti-piracy enforcement without turning internet service providers into the final arbiters of whether online content is infringing.

8 **Calcutta High Court held In-room Hotel TV broadcasts may Require Separate Copyright Licence** [9]

The Calcutta High Court considered whether hotels require a separate copyright licence when television channels carrying protected music are made available in individual guest rooms. The dispute arose because hotels typically obtain ordinary television or cable subscriptions, while copyright owners argued that making such content available as part of a commercial hospitality service amounts to a separate use under the Copyright Act, 1957.

[7] https://sansad.in/ls/committee/departmentally-related-standing-committees/12-finance-nameH=%E0%A4%B5%E0%A4%BF%E0%A4%A4%E0%A5%8D%E0%A4%A4, last accessed on August 28, 2026
[8] Home Box Office Inc. & Ors. v. Streamzy.to & Ors. (2026:DHC:5967)
[9] Hotel Appolo & Tours Private Limited v. The Indian Performing Right Society Limited (SLP(C) No. 28489/2026)

The court held that guest rooms form part of the hotel's commercial establishment and that transmission of copyrighted content to televisions installed in those rooms may amount to "communication to the public". On that basis, payment of regular television subscription charges would not, by itself, dispense with the requirement to obtain the relevant copyright licence. The Supreme Court has subsequently stayed the operation of the judgment while the challenge is pending.

The outcome will be important for hotels and other commercial accommodation providers using smart TVs, bundled entertainment services or in-room streaming systems. The final position may determine when content delivered to an individual guest remains private consumption and when its availability as part of a commercial service triggers an additional licensing obligation.

9 **Gujarat High Court held RTI-certified Copies do not Automatically become Public Documents** [10]

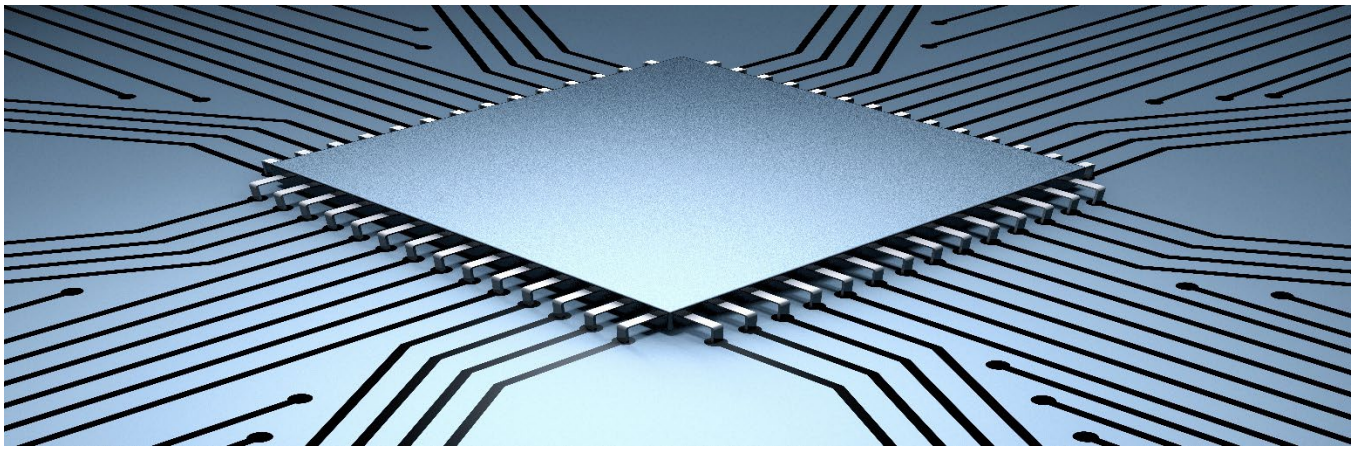
The Gujarat High Court considered the issue in a family property dispute where the plaintiffs sought to rely on two architect-issued completion certificates and a family partition agreement. Copies of these documents had been obtained from the Surat Municipal Corporation under the Right to Information Act, 2005, and the trial court had allowed them to be exhibited on the basis that they had come through a public authority.

The High Court held that the manner in which a document is obtained does not change its original character. A private document does not become a public document merely because a government authority holds a copy or furnishes it under the RTI process. A party seeking to rely on such material must still satisfy the applicable rules for secondary evidence and establish the document's authenticity and execution.

The decision is relevant as litigation increasingly relies on scanned records, digital copies and documents retrieved from government databases. An official source may establish where a copy was obtained from, but it does not by itself prove the authenticity or evidentiary value of the underlying document.

[10] Rajeshbhai Jariwala v. Falguniben Jariwala, C/SCA/17104/2021

| EUROPEAN UNION



10 **AI Act moved into Next Phase of Enforcement** [11]

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (**"AI Act"**) reached its general application stage across EU. The AI Act now governs a wider range of AI activities, including transparency requirements for certain AI systems and compliance obligations applicable to regulated AI use cases.

The AI Act, however, is still being implemented in stages. The more detailed obligations for high-risk AI systems will apply later, with different timelines depending on the category of system. Certain high-risk uses, including those relating to employment, education, biometrics and other sensitive areas, remain subject to later compliance dates, while AI systems forming part of regulated products will follow a separate timeline.

For businesses, the immediate priority is to distinguish between obligations that already apply and those that are still approaching. Organisations should classify their AI systems, identify the relevant compliance timeline for each use case and use the remaining transition periods to put appropriate governance, documentation and oversight in place.

[11] https://artificialintelligenceact.eu/article/113/, last accessed on August 20, 2026

11

Commission increased DSA scrutiny of Large Online Platforms [12]

European Commission stepped up supervisory action under Regulation (EU) 2022/2065 on a Single Market for Digital Services (**"Digital Services Act"** or **"DSA"**), seeking information from designated very large online platforms and search engines on how they are meeting their systemic risk obligations.

The scrutiny extends to the way platforms build and operate core digital features, including generative AI tools, recommender systems, user-interface choices and age-assurance mechanisms. Platforms may be required to substantiate how relevant risks were identified and mitigated through internal assessments, technical records and other supporting evidence.

The development shows that DSA compliance is increasingly reaching into product and algorithm design rather than remaining limited to content-moderation policies. Large platforms should be able to explain how recommendation models, AI features and user journeys operate, what risks were considered before deployment and whether those decisions can be supported by reliable internal records.

12

AI Office approved Guidelines for General-Purpose AI[13]

Following the enactment and phased application of AI Act, providers of general-purpose AI models are subject to specific obligations relating to transparency, copyright and information sharing with downstream providers. Models that may present systemic risks are subject to additional requirements around evaluation, risk mitigation, incident reporting and cybersecurity.

To support implementation, the General-Purpose AI Code of Practice (**"GPAI Code"**) provides a practical framework for showing how these obligations may be met in practice. It gives providers a more structured approach to areas such as model documentation, copyright-related measures, transparency around training data and, where relevant, safety and security controls for higher-risk models.

For GPAI providers, the value of the GPAI Code lies in translating broad statutory requirements into more workable compliance measures. Developers offering foundation models in the EU should therefore use it to review whether their documentation, training-data practices, copyright controls, model evaluations and cybersecurity processes are sufficiently developed to demonstrate compliance with the AI Act.

[12] https://ec.europa.eu/commission/presscorner/detail/en/mex_26_1775, last accessed on August 20, 2026
[13] https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice, last accessed on August 20, 2026

| OTHER COUNTRIES

13 **US Federal Court began examining Social Media Design and Children's Data Practices in case against Major Tech Platform**[14]

A federal court in the US commenced trial proceedings arising from consolidated claims brought by 29 state attorneys general and public-school districts against Meta Platforms, Inc. The claimants allege that features used across Facebook and Instagram, including infinite scrolling, personalised recommendation feeds and engagement-based notifications, were designed in a manner that encouraged prolonged use by children and adolescents despite alleged knowledge of potential risks associated with such engagement.

The proceedings also involve claims under the COPPA. The states allege that personal information relating to children under 13 was collected and used without the parental consent required under COPPA. The case therefore places both the design of engagement-driven platform features and the processing of children's personal data under judicial scrutiny.

The proceedings are ongoing and no final determination has been made. The case is important because its outcome could influence how social media platforms design recommendation systems and engagement features for younger users, implement age-assurance measures and use children's data for profiling or personalisation. It will therefore be important to track the trial as it progresses, particularly for businesses operating digital platforms accessed by children and teenagers.

[14] People of the State of California, et al. v. Meta Platforms, Inc., et al., Case No. 4:23-cv-05448-YGR

14

China proposed New Law on Cyberviolence and Platform Responsibility[15]

In July 2026, the CAC, along with other authorities, released the Anti-Cyberviolence Law of the People's Republic of China (Draft for Comments) (**"Draft Law"**) for public consultation. The proposal is aimed at addressing online harassment, coordinated abuse and the misuse or exposure of personal information. The consultation period closed on August 28, 2026.

The Draft Law would place wider preventive and response obligations on online platforms. These include using technical tools and human review to identify cyberviolence risks, taking action against abnormal or abusive accounts, preserving relevant evidence, restricting the spread of harmful content and complying with requirements around AI-generated content. It also places emphasis on protecting categories of personal information that may be particularly susceptible to misuse, including medical, location and other sensitive information.

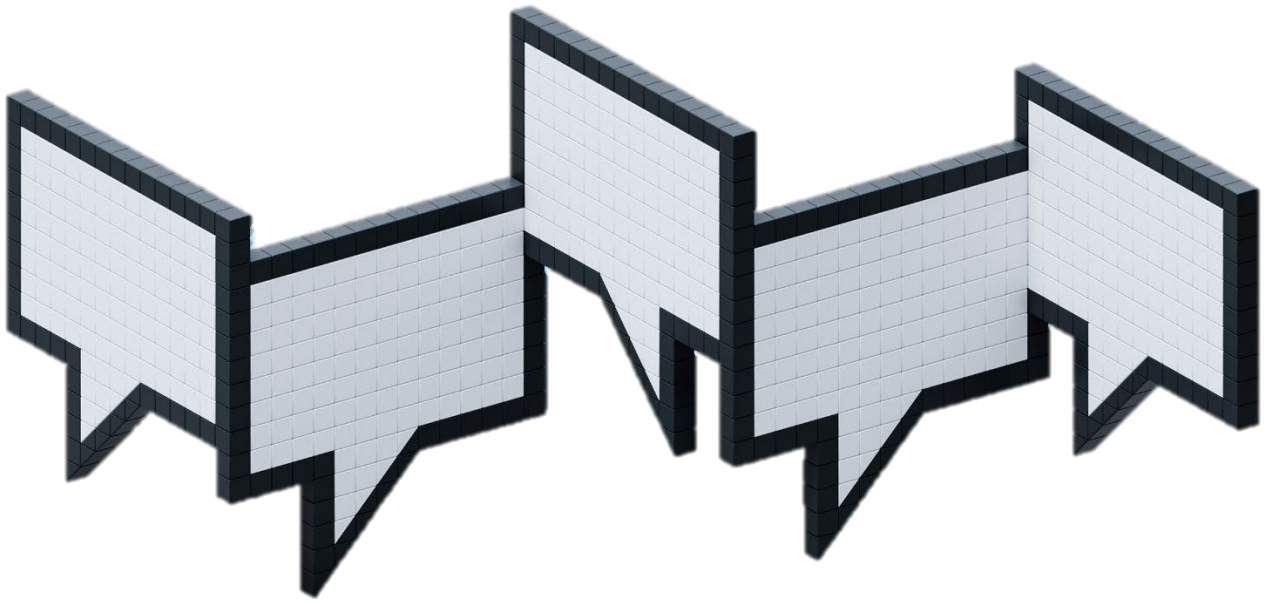
The Draft Law is important because it treats online abuse as a platform-governance and data-protection issue, not merely a content-moderation problem. If adopted, platforms operating in China may need to strengthen automated detection, account verification, evidence-retention processes and controls around the use and disclosure of personal information. The final compliance requirements will depend on the version ultimately enacted following the consultation process.

[15] https://www.cac.gov.cn/2026-07/29/c_1787072711938509.htm, last accessed on August 28, 2026

ABBREVIATIONS

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

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
CAC	Cyberspace Administration of China
COPPA	Children's Online Privacy Protection Act, 1998
DPDP Act	Digital Personal Data Protection Act, 2023
RTI	Right to Information



BEYOND THE BRIEF

People, Progress and Recent Highlights

Recent developments at Fountainhead Legal, from a growing team to timely contributions to the wider legal and regulatory conversation.

NEW TO THE FIRM

Onkar Gurav

LITIGATION COUNSEL

Brings experience across technology law, data protection and intellectual property, with a strong interest in privacy and emerging technology.

IN THE MEDIA

PERSPECTIVE

MEDIA SPOTLIGHT

AI safety, regulation and the need for stronger containment

Our Founder, Rashmi Deshpande, writing for Moneycontrol, examines why advanced AI systems need stronger containment safeguards and argues for clearer rules around safety testing, incident reporting, independent oversight and emergency shutdown mechanisms.

READ THE ARTICLE →

SME governance evolves towards technology readiness and sustainable growth

Our Partner Shirin Patel, along with Senior Associate Aarushi Ghai represented Fountainhead Legal at the SME Governance Summit 2026 at BSE, Mumbai, discussing corporate governance, technology adoption, Agentic AI, and data privacy in scaling enterprises.

READ THE POST →

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 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.

Shirin Patel, partner, is a seasoned professional with over 25 years of leadership experience in legal, compliance and governance roles within the insurance sector. Her expertise spans regulatory compliance, corporate advisory, risk and contract management, data privacy implementation and governance frameworks. She is also a qualified Company Secretary and holds a Post Graduate Diploma in Cyber Law & Cyber Forensics from the National Law School of India University.

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.

Aayush Sengupta, associate, has experience in technology law, data protection, intellectual property and dispute resolution. He is a DSCI Certified Privacy Lead Assessor and has also completed a professional course in Artificial Intelligence and Machine Learning from IIM Bhubaneswar.

Sagar Chaturvedi, associate, is a graduate of NMIMS School of Law. His experience includes banking and finance, commercial contracts, corporate law, regulatory advisory, data protection, technology law and compliance matters**.**

Onkar Gurav, Litigation Counsel, is a legal professional and qualified Company Secretary specializing in criminal law and dispute resolution. He holds a B.A. LL.B. from MNLU Mumbai and an LL.M. from NUJS, Kolkata. With extensive trial and appellate experience before the Bombay High Court, Sessions Courts, and Magistrate Courts, Onkar represents clients at Fountainhead Legal with a primary focus on criminal litigation.

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.