FOUNTAINHEAD LEGAL

FOUNTAINHEAD LEGAL

TECHNOLOGY & DATA PRIVACY BULLETIN

Insights on Technology Law, Data Protection & Digital Governance

IN INDIA	US UNITED STATES	EU EUROPEAN UNION	GB UNITED KINGDOM	OTHERS

MONTHLY EDITION **[APRIL 2026]**

FROM THE DESK OF OUR FOUNDER

FOUNDER'S NOTE

April has been a month packed with significant developments, but more than the individual updates, what stands out is the broader shift that collectively signal regulation is moving ahead even when the ecosystem is still catching up. The Online Gaming Rules being enforced while the parent legislation remains under judicial challenge, courts directing privacy disputes to a Data Protection Board that is yet to become operational, and sectoral regulators like IRDAI embedding DPDP alignment into cybersecurity expectations before the rules have fully settled these are not isolated occurrences. They reflect a simple reality that regulators are no longer waiting for the pieces to fall into place before they move. For businesses, this is a meaningful signal. The assumption that compliance timelines will be generous, or that enforcement will follow only after full clarity, is increasingly difficult to hold.

At the same time, the global conversation is beginning to move upstream. In the US, the proposed SECURE Data Act and GUARD Financial Data Act signal a shift from fragmented State regimes to a unified federal framework, bringing data-driven businesses squarely under a more direct and consistent regulatory lens.

Another major development is the growing regulatory scrutiny on data scraping. Scraping has long powered AI systems, analytics engines, and growth strategies, operating on the premise that publicly available data can be freely used. The Philippines' advisory disrupts this position. It makes it clear that public data remains regulated, and that scraping requires a lawful basis, defined purpose, and accountability in how the data is extracted. Even the method of access such as bypassing platform safeguards is brought within regulatory scrutiny.

Taken together, these developments signal a deeper shift. Data is no longer just an accessible input it is an asset that must be justified at the point of collection. For businesses, this changes the starting point of compliance. It is no longer sufficient to focus on how data is stored or protected. The question will increasingly be whether the data should have been collected at all. With that context, we hope you find this month's updates insightful.

IN THIS ISSUE

TABLE OF CONTENT

| INDIA

1 **Rules notified for Promotion and Regulation of Online Games**[1]

Government notified *Online Gaming (Promotion and Regulation) Rules, 2026* (**"Rules"**), effective from May 01, 2026, and had set up the Online Gaming Authority of India (**"Authority"**). Although, members of the Authority are yet to be nominated, the Rules provide a framework for classification, registration, user safety, and financial controls. The Authority, one formed, will review games to decide their nature within 90 days, based on factors like entry fees, deposits, chances of winning, and the revenue model. Based on this, it will determine if a game needs registration. Registration is required where the Authority considers it necessary or where the Central Government notifies certain categories, and is mandatory for e-sports.

Once registered, approval can be valid for up to 10 years but can be suspended or cancelled if the game design changes, if there is non-compliance, or if incorrect information was given. Platforms must implement user safety measures such as age gating, time limits, parental controls, and grievance systems. Banks must verify registration before allowing payments and may be directed to stop transactions for non-compliant games. Overall, the Rules increase scrutiny on both how games are designed and how money flows through them.

From an industry perspective, this comes at a time when certain industry players have already approached the Supreme Court challenging the validity of the parent legislation i.e., Promotion and Regulation of Online Gaming Act, 2025, yet the Government has proceeded to notify and operationalise the Rules from the coming month. This creates immediate compliance pressure on gaming platforms and intermediaries, even as legal uncertainty continues, requiring businesses to align with the framework while closely tracking the outcome of ongoing litigation.

[1] https://www.meity.gov.in/documents/act-and-policies/promotion-and-regulation-of-online-gaming-act-2025-and-its-corrigenda-kTMxQjMtQWa?pageTitle=Promotion-and-Regulation-of-Online-Gaming-Act,-2025-and-its-Corrigenda, accessed on April 24, 2026.

2 **Government proposed further Amendments to IT Rules, expanding Oversight of Intermediaries and AI Content**[2]

MeitY had earlier released draft amendments to the IT Rules on March 30, 2026, proposing to tighten intermediary obligations. The changes make MeitY advisories and directions binding, with possible loss of safe harbour for non-compliance. It was clarified that intermediaries may need to retain data even after takedown, extend content oversight to user-generated news, and allow the Inter-Departmental Committee to take up matters on its own. The consultation deadline, initially set for April 14, 2026 and later extended to April 29, 2026 reflects the broad impact of these proposals.

In a subsequent update, the deadline has been further extended to May 07, 2026, along with a key addition that platforms are required to ensure continuous and clearly visible labelling of AI-generated content throughout its display. This moves beyond one-time disclosures and points to persistent transparency obligations, requiring platforms to build labelling directly into how content is shown to users.

These proposed amendments will affect social media platforms, AI-driven services, and digital publishers by increasing expectations around content moderation, data retention, and AI transparency. Businesses should start evaluating the changes needed especially for continuous AI labelling and compliance with Government directions and share their feedback within the extended deadline.

3 **Revised Cybersecurity Guidelines released for Insurance Sector**[3]

IRDAI has issued amendments to the *Information and Cyber Security Guidelines Version 2.0 (April 2026)* (**"Revised Guidelines"**), introducing tighter controls on third-party and cloud risk, data handling, and governance oversight**.** The Revised Guidelines require stronger vendor and sub-outsourcing controls (including prior approvals for further outsourcing)**,** enhanced cloud service provider due diligence (including empanelment and contractual safeguards)**,** and clearer data lifecycle and deletion obligations**.** It also mandates adequate budget allocation for cybersecurity**,** along with strengthened governance through Board of Directors and committee oversight.

On the technical side, the changes introduce stricter requirements for penetration testing (via CERT-In empanelled auditors), environment parity for testing, cryptographic asset tracking, resilient backups, and segregation of infrastructure across group entities, along with tighter monitoring of third-party access and controls. The Revised Guidelines also expressly require regulated entities to align with the DPDP Regulations.

Insurers should use this as a trigger to align their cybersecurity frameworks with DPDP compliance, particularly around vendor management, data processing arrangements, and breach preparedness, where obligations are now closely interconnected.

4 **RBI released Revised Framework for Digital Payments**[4]

The RBI has issued a master direction titled *Digital Payments – E-mandate Framework, 2026* (**"Master Direction"**) with immediate effect, consolidating and updating regulatory regime for recurring digital payments (e-mandates) across cards, UPI, and prepaid instruments. The Master Direction formalises the entire lifecycle of e-mandates, including registration, execution, modification, and revocation. It requires additional authentication at the time of mandate setup, mandates advance (minimum 24-hour) pre-debit notifications, and ensures that users have the ability to opt out of individual transactions or cancel mandates altogether. It also prescribes transaction thresholds allowing recurring payments up to INR 15,000 without additional authentication (and higher limits for specified categories such as insurance and

[2] https://www.meity.gov.in/static/uploads/2026/04/ec197f1206279efb4964965f0dede6c1.pdf, accessed on April 22,2026
[3] https://irdai.gov.in/document-detail?documentId=9189223, accessed on April 22, 2026
[4] https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=13374, accessed on April 22, 2026

mutual funds) while supporting both fixed and variable mandates with user-defined caps, and strengthening post-transaction alerts and grievance redressal mechanisms.

The Master Directions also places explicit obligations on issuers, payment system providers, and acquirers to ensure compliance, including oversight of merchants and recurring payment flows. These measures align with RBI's broader regulatory approach reflected in its recent discussion paper on digital payment frauds, which emphasises user-centric safeguards and preventive controls.

Given the increase in digital payment frauds, this framework strengthens customer protection by introducing greater visibility and control over recurring debits through advance notifications, opt-out options, and authentication thresholds. For customers, this reduces the risk of unnoticed or manipulated transactions. For companies, including banks, payment aggregators, and Fintechs, it brings heightened compliance obligations, requiring upgrades to systems, real-time monitoring, and stronger oversight of merchants and recurring payment flows.

5 **Courts direct Privacy Disputes towards Data Protection Board**

Before the Kerala High Court[5], the use of facial recognition by Digi Yatra Foundation has been challenged on the ground that biometric data is being collected and processed without adequate safeguards or oversight. The court has sought a status update on the constitution and functioning of the Data Protection Board of India, highlighting the current gap in enforcement under the DPDP Regulations.

In a separate proceeding before the Indore bench of Madhya Pradesh High Court[6], a petition has challenged proposed changes to end-to-end encryption on the platform of Meta Inc. (Instagram), citing risks to user privacy and data security. The court has directed the petitioner to approach the Data Protection Board and required it to issue a reasoned decision within a defined timeline, reinforcing its role as the primary forum for such disputes.

These early cases reflect a growing focus on data privacy disputes, underscoring the need for the Data Protection Board to be fully constituted and operationalised without delay.

6 **Delhi High Court ordered Copyright Office to decide on AI-Generated Artwork Registration[7]**

Copyright Office has been ordered by the Delhi High Court to decide within 8 weeks on an application seeking registration of an artwork generated using artificial intelligence. The application had reportedly listed the AI system as the author, raising questions on whether such a claim is permissible under the Copyright Act, 1957, which recognises authorship in relation to human creators.

The case brings into focus whether works generated autonomously by AI, without direct human input, can qualify for copyright protection, and if so, who would be recognised as the rightful owner. The decision is expected to provide clarity on India's position on AI authorship.

7 **Bombay High Court refused to quash FIR in Patient Data Misuse Case[8]**

A criminal application was filed before the Nagpur Bench of Bombay High Court seeking quashing of an FIR registered under IPC and IT Act. The case involved allegations that an employee of a clinic had accessed and shared patient details with another doctor, who then used this information to divert patients and earn financial benefits. The investigation relied on material such as WhatsApp chats, call records, and

[5] CR Neelakandan v. Union of India & Ors, WP (PIL) No. 15 of 2026(S)
[6] Parth Sharma v. Union of India through Ministry of Electronics and Information and Others, WP No. 10289 of 2026
[7] Stephen Thaler v. Union of India, W.P.(C)-IPD 15/2026
[8] Dr. Utpal v. State of Maharashtra & Anr, Criminal Application (Apl) No. 1363 of 2022

financial transactions, which indicated ongoing communication and exchange of patient information between the parties.

The applicant argued that the allegations, even if accepted, would amount only to professional misconduct. The court, however, observed that the material on record suggested intentional involvement and potential financial gain, and that such intent could be inferred from the facts. As the case raised disputed factual issues requiring examination at trial, the court held that it was not appropriate to interfere at this stage and refused to quash the FIR.

This case highlights the growing risk of insider-driven data breaches, where employee access is misused to extract and share sensitive information. For corporates, this underscores the need for strong access controls, employee-level accountability, and monitoring mechanisms, especially for roles handling customer data. While the DPDP Regulations focuses on organisational safeguards, individual misconduct may still attract consequences under criminal law, making it critical for companies to address both compliance and internal enforcement risks.

8 **Karnataka High Court examined Criminal Liability of Director for Misuse of Data**[9]

In another instance involving alleged data misuse, a criminal petition was filed seeking quashing of an FIR registered under the IT Act and BNS in a dispute between co-founders of a company engaged in quantitative trading. The petitioner, a director and equal shareholder, contended that he could not be accused of data theft as the data belonged to him as part of the company. The complaint, however, alleged that he had accessed systems beyond his authorised scope, copied proprietary trading codes, deleted critical data and system logs, and misused confidential information, resulting in financial and operational harm to the company

The court rejected the argument on ownership, clarifying that company data and digital assets belong to the company as a separate legal entity, and not to individual shareholders or directors. It further noted that the allegations raised serious and complex factual issues involving unauthorised access and misuse of proprietary data, which require investigation. As such, it declined to interfere at this stage and allowed the proceedings to continue.

Disputes of this nature underline the need for robust contractual clarity on ownership and control of company data. Even founders and directors should be subject to defined access limits, confidentiality obligations, and enforceable restrictions on use and extraction of data.

9 **Anti-Money Laundering Guidelines issued for Trust and Company Service Providers**[10]

FIU-IND has issued *AML & CFT Guidelines for Trust and Company Service Providers (TCSPs)* (**"Guidelines"**) that deals with anti-money laundering and counter-terrorism financing obligations for a newly regulated class of professionals. Guidelines bring 5 activities under the PMLA when carried out in the course of business on behalf of or for another person acting as a formation agent for companies or LLPs, serving as director, secretary or partner, providing registered office or correspondence addresses, acting as trustee, and acting as a nominee shareholder. Persons performing these functions solely for their own entity are explicitly excluded.

Effective April 21, 2026, covered TCSPs must register with FIU-IND, appoint a designated director and principal officer, conduct KYC and risk-based client due diligence, screen clients daily against UNSC and UAPA sanctions lists, and file suspicious transaction reports through the FINnet portal. KYC records must be retained for 5 years and transaction records for 10 years. Employees acting for their own

[9] Aashay Harlalka v. State of Karnataka, Criminal Petition No.12927 of 2025

[10] https://fiuindia.gov.in/pdfs/downloads/AML_CFT_Guideline_TCSPs.pdf, accessed on April 28, 2026

employer, and professionals filing incorporation declarations in a limited capacity, are carved out from the scope.

10 **Gujarat High Court released Policy on Use of AI in Judicial and Court Administration**[11]

A comprehensive policy entitled *Policy on Use of Artificial Intelligence Tools in Judicial and Court Administration,* (**"AI Policy"**) has been released by Gujarat High Court. It sets out clear boundaries on how AI may be used by judges, court staff, and law clerks, permitting its use only as an assistive tool and prohibiting any reliance on AI for judicial reasoning or decision-making. It restricts the use of cloud-based AI services without explicit approval to safeguard the confidentiality of court proceedings. Judges are required to verify all AI-generated outputs and maintain audit records of AI usage. The AI Policy follows a similar framework introduced by the Kerala High court in July 2025, and signals a growing consensus across the Indian judiciary on the need for structured AI governance within court systems.

11 **Government formed AI Governance Group**[12]

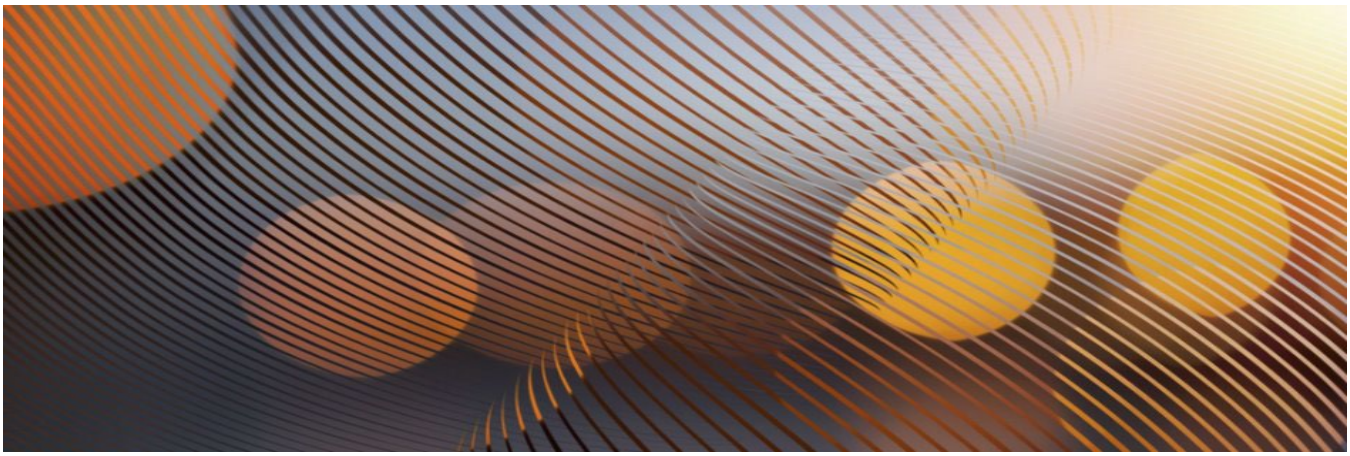
A committee titled *AI Governance and Economic Group (AIGEG)* (**"Committee"**) has been formed with an aim of having a coordinated national approach to AI governance and economic impact. The Committee has been given the task to look into areas such as aligning policies across ministries and regulators, reviewing existing laws to ensure accountability of firms, identifying regulatory gaps, and recommending legal changes. It will also assess AI use cases and classify them based on readiness, develop a roadmap for AI deployment, study risks, and evaluate the impact on jobs, including planning for workforce transition and skill shifts.

From an industry perspective, this signals a move toward more structured oversight of AI systems, with a focus on accountability and compliance with existing laws. Companies may see clearer guidance on acceptable AI use, but also increased expectations around risk assessment, transparency, and alignment with national priorities. The focus on labour impact and job transitions indicates that sectors adopting AI at scale may face closer scrutiny, especially where automation affects employment. Overall, this is an early step toward a more formal AI regulatory framework, with implications for both innovation strategy and compliance planning.

[11] https://gujarathighcourt.nic.in/hccms/sites/default/files/miscnotifications/Policy%20on%20the%20use%20of%20Artificial%20Intelligence%20in%20the%20Judicial%20and%20Court%20Administration.pdf, accessed on April 21, 2026

[12] https://www.meity.gov.in/static/uploads/2026/04/43a4ec455c26b0f061cc7cca98770a45.pdf, accessed on April 21, 2026

| UNITED STATES OF AMERICA



12 **Congress introduces Landmark Bills to Overhaul Data Privacy Regime**[13]

House Energy & Commerce Committee and the House Financial Services Committee jointly introduced the *Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act* (**"SECURE Data Act"**) and the *Guidelines for Use, Access, and Responsible Disclosure of Financial Data Act* (**"GUARD Financial Data Act"**), the most significant federal push on data privacy in decades. The SECURE Data Act establishes a national framework giving consumers control over their personal data, and to opt out of targeted advertising, data sales, and automated profiling while GUARD Financial Data Act modernises the 26-year-old Gramm-Leach-Bliley Act, 1999 restricting financial institutions to collecting only data that is necessary for the service provided, and introducing new rights for current and former customers to access and delete their financial data.

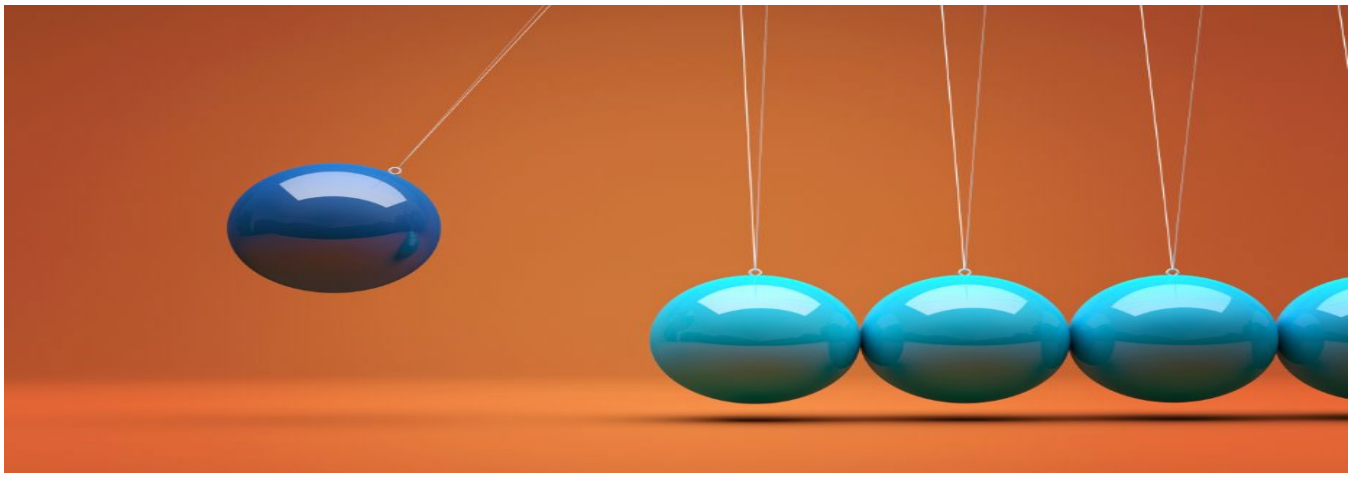
The SECURE Data Act introduces heightened protections for sensitive data including health information, biometrics, location, data relating to race, religion, and immigration status requiring explicit consumer consent before any collection or disclosure. It applies to businesses collecting data of more than 200,000 consumers annually with revenues of USD 25 million or more, or those collecting data of more than 100,000 consumers where 25% or more of revenue derives from data sales. Processing data of teenagers between 13 and 15 requires verifiable parental consent, and automated decisions with legal or significant consequences must be disclosed in advance with a right to opt out.

The GUARD Financial Data Act, on the other hand, focuses on the financial sector specifically. It requires affirmative opt-in consent before sensitive financial data can be collected or shared with third parties. Financial data aggregators and third-party applications accessing consumer bank accounts through login credentials would face strict new notice and consent requirements. It extends special consideration to smaller financial institutions with assets of USD 15 billion or less, directing regulators to account for their resource and personnel limitations when prescribing compliance regulations.

These bills mark a turning point. If passed, US would have a single federal privacy standard ending years of fragmented state-by-state compliance. But the shift is not merely structural. Both bills place the burden on businesses to act proactively, not reactively. Companies that collect, process, or profit from personal data should treat the introduction of these bills as a compliance trigger, not a waiting signal.

[13] https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=411100, accessed on April 27, 2026

| EUROPIAN UNION



13 **Regulators seek Feedback on Responsible Chatbot Use**[14]

Netherlands Authority for Consumers and Markets (ACM) and the Dutch Data Protection Authority (AP) have invited inputs on the responsible use of chatbots in customer service and citizen interactions, until May 17, 2026. The consultation has been launched due to growing concerns around reduced human interaction, lack of transparency in chatbot usage, risks of misleading responses, and privacy issues arising from increased reliance on AI-driven interfaces. The regulators are working together to issue practical guidelines covering areas such as disclosure, accessibility to human support, reliability of responses, and data security.

From an industry perspective, this comes ahead of new rules that will begin applying in phases under the EU AI Act. Stakeholders can use this opportunity to shape how these requirements are interpreted in practice by highlighting real-world challenges and suggesting workable standards.

14 **Draft Standards for Health Data Sharing released for Feedback**[15]

European Commission has invited feedback on a draft regulation under the European Health Data Space (EHDS), with the consultation open till May 12, 2026. The proposal focuses on how health datasets should be described before they are shared for research or other secondary uses. It requires data holders to provide clear and standardised information about their datasets, such as what the data contains, where it comes from, how it can be accessed, coding systems used, presence of personal data, number of records or individuals, time period covered, conditions for access etc. The aim is to create standardised, machine-readable dataset catalogues that can be linked across Member States to enable easier discovery and reuse of health data.

[14] Call from ACM and AP: please share your opinion on chatbots in customer service | ACM, accessed on April 27, 2026
[15] European Health Data Space – dataset descriptions, accessed on April 27, 2026

| UNITED KINGDOM

15	**Privacy Regulator issues Draft Guidance on Automated Decision-Making in Recruitment**[16] ICO has issued draft guidance clarifying the scope of automated decision-making (ADM) under the UK GDPR focusing on recruitment practices. It reiterates that individuals have the right not to be subject to decisions made solely through automated processing where such decisions have legal or similarly significant effects. ADM is permitted only in limited cases such as where it is necessary for contract performance, authorised by law, or based on explicit consent and must be accompanied by safeguards, including human intervention, the ability to challenge outcomes, and transparency around the logic involved. In parallel, the ICO's *"Recruitment Rewired"* report highlights concern around the growing use of AI-driven hiring tools without adequate transparency or meaningful human oversight, increasing risks of bias and exclusion. Together, these signal a clear regulatory direction toward stricter scrutiny of algorithmic decision-making. Businesses particularly those using AI in hiring should proactively reassess their systems for explainability and genuine human involvement, especially where they have UK-facing operations.

[16] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/03/here-s-what-jobseekers-need-to-know-about-automated-recruitment-decisions/, accessed on April 27, 2026

| OTHER COUNTRIES

16 **Philippines – Advisory issued on Public Data Scrapping**[17]

NPC has issued *Guidelines on Data Scraping of Publicly Available Personal Data (NPC Advisory No. 2026-01)* (**"Advisory"**) that deals with data scraping (the automated or manual extraction of personal data from websites and online platforms into structured formats such as databases). The Advisory firmly establishes that publicly available personal data is not exempt from the Data Privacy Act, 2012. Organisations that scrape data must identify a lawful basis for processing, issue a privacy notice to affected individuals, conduct a Privacy Impact Assessment, and collect only what is strictly necessary for a declared purpose. Scraping sensitive personal information or data of vulnerable individuals such as minors requires significantly higher justification, and circumventing anti-scraping measures like CAPTCHAs or robots.txt is explicitly deemed unauthorised, carrying criminal, civil, and administrative liability.

Website operators hosting publicly available data are equally in scope and must inform users of potential scraping, monitor for bot activity, enforce rate limits, and treat unauthorised scraping as a notifiable data breach where applicable. For businesses across ASEAN that rely on web-sourced data for AI training or analytics, this Advisory is a clear signal that the region is closing the 'publicly available' loophole, and compliance frameworks must be updated accordingly.

17 **China – Government introduced Voluntary Measures for Cybersecurity Labels**[18]

CAC, Ministry of Industry and Information Technology, and Ministry of Public Security have jointly issued the *Measures for the Administration of Network Security Identification* (**"Measures"**) that deals with a formal cybersecurity labelling system for internet-connected products in China. The Measures establish the 'China Cybersecurity Label', a voluntary scheme under which product manufacturers may certify and display a star-rated security label with one-star for products meeting basic national security standards such as eliminating weak passwords and maintaining vulnerability patches, two-star for products demonstrating advanced security capabilities, and three-star for market-leading products that

[17] https://privacy.gov.ph/wp-content/uploads/2026/04/SGD_A_1.pdf , accessed on April 28, 2026
[18] https://www.jswx.gov.cn/fwhd/tzgg/202604/t20260410_1322303.shtml , accessed on April 28, 2026

additionally pass rigorous penetration testing. Manufacturers must obtain independent test reports, register with the designated filing authority, and display the label only after formal approval, which must be completed within ten working days of a complete submission.

While participation is voluntary, the Measures carry significant commercial weight as regulators explicitly encourage consumers to prefer labelled products, creating a de facto market incentive for compliance. Misuse of the label, including forgery, false advertising, or submitting fraudulent test reports, results in immediate deregistration, a one-year ban from re-application, public disclosure of violations, and penalties under the cybersecurity law, with misconduct recorded in national credit information system. Effective July 1, 2026, businesses manufacturing or selling internet-connected devices in China should assess whether their products fall within the published product catalogue and begin aligning their security architecture and testing processes with the applicable tier requirements ahead of the deadline.

18 **China – Government introduced Interim Measures on Humanised AI Interactive Services**[19]

CAC, along with key regulations has issued Interim Measures for the Administration of Humanized Interactive *Services Based on Artificial Intelligence* (**"Interim Measures"**), that are effective July 15, 2026. The Interim Measures establish a governance framework for AI systems designed to simulate human-like interaction. These apply to services such as AI companions for elderly care, virtual tutors for children, conversational digital avatars, and emotionally responsive chatbots used in cultural or social settings. The Interim Measures aim to balance innovation with risk mitigation by introducing baseline compliance obligations. The framework also mandates security assessments, algorithm filing requirements, and risk controls for high-impact systems, while encouraging responsible innovation through sandbox mechanisms. Overall, the regulation reflects China's increasing focus on ethical and safety risks arising from anthropomorphic AI, particularly in sensitive, high-trust user environments.

[19] https://www.cac.gov.cn/2026-04/10/c_1777558395023172.htm , accessed on April 28, 2026

ABBREVIATIONS

The following abbreviations are used throughout this newsletter.

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
BNS	Bharatiya Nyaya Sanhita, 2023
CAC	Cyberspace Administration of China
DPDP	Digital Personal Data Protection
FIU-IND	Financial Intelligence Unit – India
ICO	Information Commissioner's Office
IRDAI	Insurance Regulatory and Development Authority of India
IT Act	Information Technology Act, 2000
IT Rules	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
IPC	Indian Penal Code, 1860
LLP	Limited Liability Partnership
MeitY	Ministry of Electronics and Information Technology
NPC	National Privacy Commission
PMLA	Prevention of Money Laundering Act, 2002

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.