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 **[JULY 2026]**

FROM THE DESK OF OUR FOUNDER

FOUNDER'S NOTE

The most arresting update this month began not with a judgment, but with a notice to a code-hosting platform. The Indian Cyber Crime Coordination Centre reportedly asked GitHub to disable repositories linked to BitChat, a messaging tool that can operate through Bluetooth without internet access or a central server. The attention came from what the direction sought to restrict: not an unlawful message or a particular user, but the source code from which the technology could be built. It also relied on the intermediary takedown route rather than the usual website-blocking process. That distinction matters because open-source code may serve legitimate purposes, may already have been copied or modified, and cannot always be contained by removing it from one platform. The episode has therefore opened a wider discussion on whether rules designed for online content can be applied in the same way to the technology that enables communication.

A similar question appears in the debate on web scraping, although in a setting far more familiar to businesses. Collecting information from publicly accessible websites is now part of activities ranging from market research and price monitoring to lead generation, data analytics and AI development. The draft European guidance and the Singapore AI guidelines challenge the common assumption that information visible online is automatically free to collect and reuse. Businesses may still need to explain what was collected, why it was necessary, whether access restrictions were ignored and how individuals were informed. The issue becomes more difficult where a company buys a dataset from a vendor, because a commercial licence does not necessarily establish that the underlying collection was lawful.

The Delhi High Court's interim order in the AI copyright dispute adds another layer. The court declined to restrain the use of news material for model training on the evidence before it, but did not finally decide that all training on publicly available content is lawful. The source of the material, the manner of collection, the likelihood of reproduction and evidence of market harm may still shape the final outcome. Read with the web-scraping and blockchain developments, the larger message is that businesses must understand where their data came from and what happens to it once it enters a model or technical architecture. A privacy notice or contract prepared later may not resolve a problem created at the point of collection or design.

The Indian regulatory updates brought the same operational focus into more established sectors. The RBI's draft guidance expects boards and management to take ownership of data quality and access. The CBDT's crypto-asset reporting framework depends on accurate links between customer onboarding, tax information and transaction records. CDSCO's guidance places validation, cybersecurity, algorithm changes and monitoring within the lifecycle of medical software. The CCPA's dark-pattern order shows that even the smallest design decision, such as a pre-selected checkbox, can carry legal consequences where it influences a consumer's choice.

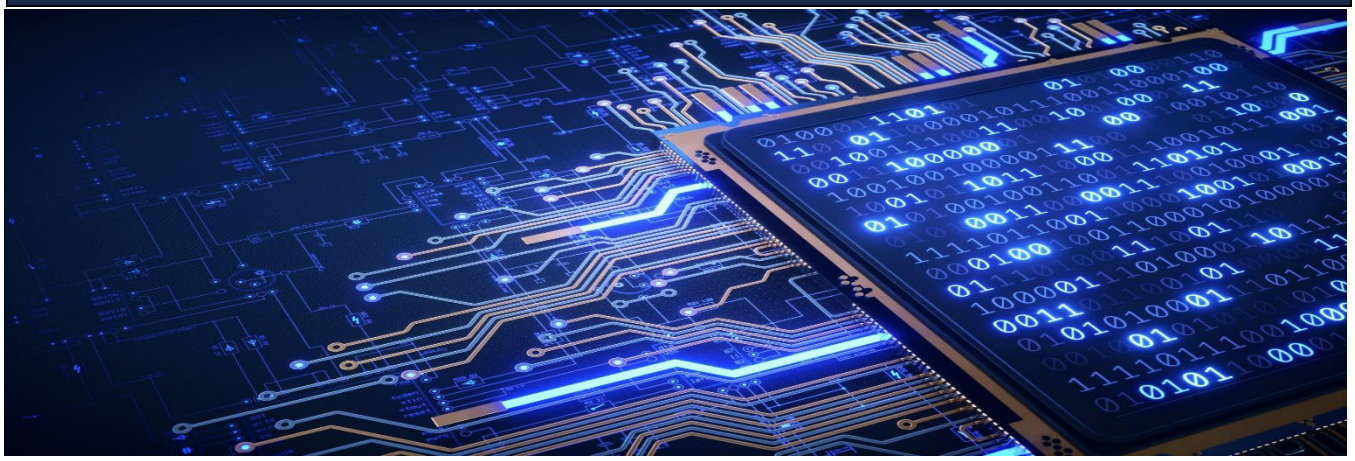
The account-freezing decisions and the removal of battery-management applications show why the manner of intervention matters just as much as the reason for it. A restriction may be justified where there is fraud, safety risk or serious misuse, but its scope must remain connected to the actual harm. This month's developments leave businesses and regulators with the same practical question: are we acting at the right point in the technology, and is the response precise enough to solve the problem without creating a larger one?

We hope you find this edition insightful!

IN THIS ISSUE

TABLE OF CONTENTS

| INDIA



1 **RBI released Draft Guidance on Data Governance**[1]

On July 15, 2026, the RBI released the draft *Guidance on Regulatory Expectations for Data Governance* (**"Draft RBI Guidance"**) for public comments. The consultation remains open until August 17, 2026. The Draft RBI Guidance is for banks, NBFCs and other regulated entities (**"REs"**) and expects each RE to establish a comprehensive data governance framework covering the manner in which data is identified, classified, accessed, maintained, shared and governed across its lifecycle. Oversight is expected at the highest level, with the Board of Directors responsible for approving the framework and Data Governance Committees operating at the board and executive levels.

The Draft RBI Guidance also places clear responsibility on identified personnel. Data Owners are expected to remain accountable for data within their business domain, Data Stewards for quality and appropriate use, and Data Custodians for technical storage, security and availability. The framework therefore moves data governance beyond the information technology function and requires business teams, risk, compliance and technology teams to work within a common ownership structure. Data quality, integrity and classification are particularly important because regulatory reports, risk models, customer decisions and management information all depend on reliable underlying data.

Third-party arrangements receive specific attention. Access to shared data should be limited to persons with a genuine need to know, and appropriate confidentiality obligations should be included in contracts. REs will therefore need visibility over what data is shared with service providers, who can access it, the purpose for which it is used and the controls applied throughout the arrangement.

The Draft RBI Guidance makes data governance a board and management responsibility rather than a policy exercise. REs should now assess whether their data inventory, ownership matrix, access controls, quality checks and vendor arrangements can be demonstrated through records and audit trails. The same work will support DPDP compliance, but the two frameworks should be implemented together rather than through separate and duplicative programmes.

[1] https://rbidocs.rbi.org.in/rdocs/Content/PDFs/DATAGOVERNANCE150720269AC6EBBBC8A84C9D902EF886D9219AA9.PDF, last accessed on July 16, 2026

2	**CBDT issued Guidance Note on Crypto-asset Reporting Obligations**[2] CBDT published *Crypto-Asset Reporting Obligations under Section 509 of the Income-tax Act, 2025: Guidance Note* (**"Guidance Note"**). The Guidance Note explains the reporting obligations under Section 509, Rules 241 to 244 and Form 167 of the Income-tax Rules, 2026, which have been in force since April 01, 2026. The Guidance Note is intended to support implementation of the OECD Crypto-Asset Reporting Framework (**"CARF"**) and increase tax transparency in relation to crypto-asset transactions. The Guidance Note requires Reporting Crypto-Asset Service Providers (**"RCASP"**) to determine whether they fall within the reporting regime, identify reportable users and transactions, undertake prescribed due diligence and furnish the required information to the income-tax authorities. It also addresses the correction of inaccurate statements and enables the Government to prescribe requirements relating to registration, record maintenance and identification of crypto-asset users or owners. Non-compliance may result in daily penalties for delayed reporting and separate penalties for inaccurate information or failure to meet the due-diligence requirements. The obligation is operationally significant because accurate reporting depends on information collected much earlier in the customer lifecycle. Customer onboarding, tax-residency information, account classification, transaction records and wallet or platform data must be capable of being connected and validated. Errors in source data may therefore flow directly into regulatory reporting and expose the RCASP to repeated corrections or penalties. *For crypto businesses, reporting under CARF is not merely a year-end tax filing exercise. It requires continuing data governance across onboarding, transaction monitoring, record retention and regulatory reporting. RCASPs should identify ownership between tax, compliance, operations and technology teams and ensure that the larger volume of reportable customer data is protected through appropriate access and security controls.*

3	**Delhi High Court refused Interim Injunction in Copyright Dispute involving AI Training**[3] In *ANI Media Pvt. Ltd. v. OpenAI OpCo LLC*, the Delhi High Court dismissed ANI Media Private Limited's (**"Applicant"**) application for an interim injunction against OpenAI Inc. (**"Respondent"**). Applicant had alleged infringement on two broad grounds: first, that its copyrighted news material had been copied and stored for training the large language models underlying 'ChatGPT', and second, that responses generated by ChatGPT reproduced or closely resembled Applicant's protected content. The Applicant sought restraints on the use of its works and related interim relief while the suit remained pending. The court first held, on a prima facie basis, that it had territorial jurisdiction. Although Respondent stated that model training and storage took place on servers outside India, the alleged responses were generated for users in India and formed part of the same chain of events as the training claim. The court therefore declined to treat the foreign location of the servers as sufficient to exclude the application of Indian copyright law at the interim stage. On the merits, the court found that Applicant had not shown substantial reproduction of its articles, memorisation of its works or regurgitation of protected content through the examples placed on record. It also took a prima facie view that Respondent's temporary storage and use of Applicant's literary works for model training satisfied the purpose and fairness tests under the fair-dealing exception in the Copyright Act, 1957. The court noted, among other factors, that the material was obtained from freely accessible

[2] https://www.incometaxindia.gov.in/documents/d/guest/e-book-guidance-note-crypto-asset-reporting-obligations-pdf, last accessed on July 29, 2026
[3] ANI Media Pvt. Ltd. v. OpenAI OpCo LLC, CS(COMM) 1028/2024

sources, the model was not designed to reproduce the training material, the outputs were not substitutes for Applicant's news articles and no evidence of actual market loss had been produced.

The court further held that the balance of convenience and public interest did not support a blanket injunction. Applicant's claim was capable of monetary assessment if it ultimately succeeded, while an injunction could materially affect Respondent's functioning and users of the service. Importantly, the court expressly clarified that these findings were limited to the interim application and would not determine the final outcome of the suit.

The order is an important interim indication, not a final ruling that all AI training on publicly available content is lawful. Its reasoning is closely tied to the evidence placed before the court, the source and manner of collection, the nature of the generated outputs, evidence of memorisation and market harm. AI developers and content businesses should therefore continue to maintain records of training sources and opt-out controls, output safeguards, licensing positions and the commercial impact of model use.

4 **Parliamentary Committee recommended Interim Framework for VDA**[4]

Parliamentary Standing Committee on Finance adopted the *Thirty-Sixth Report on the Securities Markets Code, 2025* (**"Report"**), which was presented to the Lok Sabha and laid in the Rajya Sabha on 23 July 2026. In the Report, the Committee recommended that the Government establish a regulatory framework for VDAs. Recognising that a comprehensive framework may take time, it suggested that an interim mechanism be considered to address the current regulatory gap.

The Report proposed that the interim regime could operate through Self-Regulatory Organisations (**"SROs"**). Such bodies could prescribe standards relating to governance, transparency, disclosures and compliance with a code of conduct. The recommendation is intended to reduce the risks created by the absence of a single operating framework, even though VDA businesses are already subject to tax, anti-money-laundering and other legal requirements.

An SRO-led model could give the sector more immediate standards and a forum for supervision, but its effectiveness will depend on membership, oversight, enforcement powers and coordination with existing regulators. It also would not resolve all questions relating to investor protection, custody, market conduct or the legal treatment of different crypto-assets.

Exchanges, custodians and other VDA service providers should not treat the absence of a final statute as an absence of regulatory expectation. Governance, customer disclosures, asset segregation, complaint handling and transaction records are likely to remain central under either an interim or final regime. Businesses should therefore build controls that can be adapted rather than waiting for the final architecture to be announced.

5 **CCPA penalised Airline for Dark Patterns in Online Booking**[5]

In its final order in the matter of SpiceJet Limited (**"Company"**), CCPA imposed a penalty of INR 1 Lakh after taking suo motu cognisance of practices on its online booking portal. CCPA found that consumers booking tickets were automatically enrolled in the 'Spice Club' loyalty programme through a pre-ticked checkbox. The design required a consumer to identify and remove the selection instead of making an active choice to join.

The CCPA classified the practice as involving forced action, interface interference and a trick question under the Guidelines for Prevention and Regulation of Dark Patterns, 2023. It also noted that after receiving

[4] https://sansad.in/getFile/app/lsscommittee/Finance/18_Finance_36.pdf?source=app , last accessed on July 29, 2026
[5] https://ccpa.doca.gov.in/checkuploaddocs.php?updocs=./uploads/SpiceJetLt.pdf&unique_id=, last accessed on July 29, 2026

notice, the Company replaced the loyalty-programme selection with another pre-ticked checkbox for promotional communication through SMS, WhatsApp and email. CCPA did not accept the explanation that the design resulted from a technical error and treated the conduct as a misleading advertisement, an unfair trade practice and an unfair contract under the Consumer Protection Act, 2019.

Airlines, e-commerce businesses and digital platforms should review the complete customer journey, including loyalty enrolment, marketing permissions, add-ons and ancillary services. Product acceptance and permission for promotional communication should be separate, equally visible and based on a clear affirmative action. This approach also aligns closely with the consent standard under the DPDP framework.

6 **Government ordered Removal of Battery Management System Applications from App Stores**[6]

The Government took note of reports that certain Battery Management System (**"BMS"**) mobile applications allowed unauthorised remote control of e-rickshaw batteries. On July 03, 2026, it issued orders directing app stores to remove the identified applications (**"Removal Orders"**). The concern was not confined to misuse of software, remote interference with a battery could create a direct risk to vehicles, drivers, passengers and public safety.

In its response, the Government also referred to the national cybersecurity framework, including the National Cyber Security Coordinator, the CERT-In, the National Cyber Coordination Centre and the National Critical Information Infrastructure Protection Centre. The matter therefore illustrates how connected-device risks may involve product safety, cybersecurity, consumer protection and platform responsibility at the same time.

Where a vulnerability threatens public safety, regulators may move beyond directing remediation and require the application or service to be removed. Businesses operating connected products should therefore treat cybersecurity as part of product governance and safety approval, not merely as an information-technology control.

7 **Madhya Pradesh High Court allowed Release of Account Frozen in Cyber-fraud Investigation**[7]

In a recent matter, the Madhya Pradesh High Court considered bank accounts frozen on the basis of communications received from different cybercrime cells. The petitioner stated that it had not been informed of any alleged involvement in cybercrime and that the freeze had been imposed without the investigating agency completing the process required before the competent Judicial Magistrate.

The court held that an account could not remain frozen indefinitely merely on the basis of communications from cybercrime authorities where the procedure under the BNSS had not been followed. It directed the bank to release the accounts while requiring the disputed amount to be placed in a fixed deposit for three months, subject to any further direction from the competent Magistrate after the investigation.

The order protected the disputed amount without allowing an open-ended restriction over the petitioner's complete banking operations. It also reinforced the need for investigating agencies and banks to document the legal authority, procedural steps, amount under dispute and continued necessity of each freeze.

The decision forms part of a wider judicial concern with indefinite and account-wide restrictions arising from cyber-fraud complaints. Banks should periodically review freezes instead of treating an initial

[6] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2287651&reg=48&lang=2
[7] Dekain Perfect Tech Ksolution Private Limited v. IDFC First Bank & Ors., Writ Petition No. 18579 of 2026

communication as a permanent direction. A targeted hold can preserve funds for an investigation without unnecessarily paralysing a legitimate business.

8 **Andhra Pradesh High Court ordered Defreezing of Account frozen over INR 1,000 UPI Transaction**[8]

In a recent matter, Andhra Pradesh High Court directed the State Bank of India to defreeze the current account of a licensed wine retailer. The account had been frozen after it received INR 1,000 UPI payment from a person who was subsequently accused of cheating in Bihar. No prior notice or reason was given to the petitioner, and a communication explaining the freeze was issued only after the petitioner made enquiries.

The restriction affected the entire balance of INR 8,26,633 and prevented the petitioner from using its operating funds. The court observed that a small merchant accepting payments through services such as PhonePe or Google Pay cannot ordinarily verify the credentials or background of every customer. There was no material showing that the petitioner was involved in the alleged offence or had any connection with the accused beyond receiving the disputed payment.

Against this background, the court held that freezing the complete account without examining the petitioner's role was unlawful and directed the bank to restore access. The case reflects the serious commercial consequences that may follow when a small disputed transaction results in an account-wide restriction.

Cyber-fraud response must be effective, but it should also be proportionate. Where the account holder is not implicated, banks and investigating agencies should consider ring-fencing the disputed amount rather than disabling the entire account. Businesses should retain transaction records and maintain escalation channels so that the basis, scope and duration of a freeze can be challenged promptly

9 **CDSCO issued Final Guidance on Medical Device Software**[9]

CDSCO issued the final *Guidance Document on Medical Device Software, Doc. No. SCO/MD/GD/MDSW/01/2026* (**"Guidance"**). The Guidance explains how the Medical Devices Rules, 2017 apply to software intended for medical purposes, including standalone software, embedded software, mobile applications, cloud-based platforms and AI or machine learning tools. It is clarificatory and does not create a separate regulatory regime.

Whether a product qualifies as Medical Device Software will depend mainly on its intended use and actual functionality. Software used for diagnosis, screening, monitoring, treatment, prediction or clinical decision-making may fall within the framework, while general wellness, administrative, billing, communication and data-storage tools may remain outside it unless they perform a medical function. The Guidance also addresses risk classification, licensing, clinical evidence, quality-management systems, cybersecurity, AI bias and drift, software updates and post-market monitoring.

The Guidance makes product design and positioning a regulatory issue. Health-tech businesses should assess early whether their software performs a medical function and ensure that licensing, validation, cybersecurity, data protection and post-market controls are built into the product lifecycle before launch.

[8] Sri Sai Wines v. Union of India & Ors., Writ Petition No. 969 of 2026

[9] https://cdsco.gov.in/opencms/export/sites/CDSCO_WEB/Pdf-documents/Guidance-document-on-Medical-Device-Software-under-MDR-2017.pdf , Last accessed on August 01, 2026

10 **BCI issued Circular on Social Media, AI Use and Digital Conduct for Advocates and Law Students**[10]

BCI issued a circular covering the use of social media, court-related content and generative AI by advocates, law students, interns, law firms and chambers. It cautions against recording inside court premises, sharing confidential client or chamber material, using legal content for indirect solicitation, making claims of influence or assured results, circulating fabricated judgments and publishing misleading AI-generated or deepfake content. Educational and public-awareness content remains permissible, provided it is accurate, restrained and non-promotional.

The circular also envisages affidavits at enrolment, undertakings from students and interns, Digital Ethics Committees, complaint portals and coordinated requests to online platforms. Depending on the nature of the breach, consequences may include removal or correction of content, disciplinary proceedings, reporting to courts, withdrawal of internships and other legal action. It operates immediately as an advisory and implementation framework while formal rule changes are considered.

This circular is significant as it treats online conduct as an extension of courtroom and client-facing duties. Law firms and advocates should therefore review approval processes for social-media content, protect confidential information and clearly identify AI-generated material before publication.

[10] https://www.barcouncilofindia.org/info/forwarding-d4cwwl , Last accessed on August 03, 2026

| EUROPEAN UNION

11 **EDPB issued Draft Guidelines on Web Scraping for Generative AI**[11]

EDPB released the *Guidelines 03/2026 on web scraping in the context of generative AI* (**"Draft Web Scraping Guidelines"**) for public consultation. The consultation period is till October 31, 2026. The Draft Web Scraping Guidelines remain a draft and do not have an effective date. They cover situations where an AI developer scrapes personal data from external internet sources itself, appoints another party to do so or obtains an existing scraped dataset for model training or fine-tuning. They make clear that responsibility must be assessed on the basis of each organisation's actual role in determining the purpose and manner of collection and reuse.

The central position is that public availability does not remove the application of the GDPR. Organisations must identify a lawful basis, define a specific purpose and comply with fairness, transparency, data minimisation and accuracy. Legitimate interests may be available, but only where the interest is legitimate, the processing is necessary and the balancing test does not favour the individual. Large-scale collection without the individual's knowledge, together with the possibility of model memorisation or inference, is treated as a significant risk.

EDPB proposed controls before and after collection. These include considering synthetic data, defining precise collection criteria, excluding websites or categories that are unnecessary or oppose scraping, applying filters, using reliable sources, time-stamping and validating data, and deleting, anonymising or pseudonymising personal data as early as possible. Special-category data requires a separate exception under the GDPR. Where individual notice is impossible or disproportionate, the organisation must still provide accessible public information about the categories, purposes, legal basis and sources of data.

The Draft Web Scraping Guidelines are equally relevant where a business buys a ready-made dataset. Purchasing from a vendor does not answer whether the original scraping was lawful or whether the buyer's reuse has its own legal basis. AI developers should therefore maintain source records, collection

[11] https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_2020603_webscraping_v1_en_0.pdf , last accessed on July 29, 2026

criteria, exclusion lists, legitimate-interest assessments, transparency notices and controls against memorisation and regurgitation.

Data sourcing is becoming a core governance question for AI. A model may be technically effective yet legally exposed if the business cannot explain where the training data came from and why its collection and reuse were lawful. Vendor due diligence must therefore examine the provenance of the dataset, not merely its quality and commercial licence.

12 **EDPB adopted Guidelines on Personal Data and Blockchain Technology**[12]

EDPB adopted the final version of the *Guidelines 02/2025 on processing of personal data through blockchain technologies* (**"Blockchain Guidelines"**). The Blockchain Guidelines explain how the technical design of a blockchain affects the allocation of controller and processor roles, compliance with GDPR, international transfers and the exercise of individual rights.

The Blockchain Guidelines advise organisations to avoid storing personal data directly on-chain unless the purpose strictly requires it. They recommend alternatives such as keeping data off-chain and recording only a reference, using encryption, keyed hashing or cryptographic commitments and limiting the information visible to network participants. The choice of architecture, governance model and access permissions must be assessed before deployment, not after personal data has been written to an immutable ledger.

A Data Protection Impact Assessment is required where the processing is likely to create high risk. Organisations must also consider whether blockchain is necessary for the proposed use and whether the system can support obligations relating to accuracy, storage limitation, rectification, erasure and security. The existence of multiple participants does not remove the need to identify who determines the purposes and means of processing.

Blockchain's defining feature of immutability can conflict directly with data-protection requirements. Businesses should therefore resolve privacy questions at the architecture stage and document why blockchain is preferable to a conventional database. Once identifiable information has been placed permanently on-chain, a privacy policy or contractual clause may not be capable of correcting the design.

13 **CJEU limited Journalistic Exemption for Commercial Criminal-record Databases**[13]

CJEU held that placing criminal-conviction decisions in a paid and searchable online database does not, by itself, amount to processing for "journalistic purposes" under GDPR. The dispute arose after the operator of a Swedish database refused to erase information relating to an individual who had been convicted in 2011.

The operator argued that Swedish constitutional protection for the database excluded the application of the GDPR and left the individual only with a possible defamation remedy. The CJEU rejected the possibility of such a broad exclusion. Member States may create derogations to reconcile data protection with freedom of expression, but only where the processing genuinely serves a journalistic, academic, artistic or literary purpose.

The court stated that relevant factors include whether the activity aims to communicate information, opinions or ideas to the public, whether the material is edited or adapted under an editorial policy, whether professional or ethical standards are followed and whether factual allegations are verified. A commercial database that simply republishes public criminal decisions in a searchable format cannot assume that it falls within the exemption.

[12] https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202502_blockchain_v2_en.pdf , last accessed on July 30, 2026
[13] https://curia.europa.eu/site/upload/docs/application/pdf/2026-07/cp260100en.pdf , last accessed on July 30, 2026

The judgment is relevant to legal-information platforms, background-screening services and other businesses that commercialize public records. Public source material remains personal data, and the legal position depends on the purpose and manner of reuse. Operators should assess editorial involvement, retention periods, searchability and the handling of erasure or objection requests instead of relying only on the public nature of the underlying record

| OTHER COUNTRIES

14 **Singapore – Privacy Commission issued Guidelines on Personal Data in Generative AI**[14]

PDPC issued *Advisory Guidelines on Use of Personal Data in Generative AI* (**"AI Guidelines"**), explaining how the Personal Data Protection Act, 2012 applies across the development, deployment and post-deployment stages of generative AI and clarify the responsibilities of model providers, system providers and organisations deploying the technology.

A key part of the AI Guidelines addresses personal data collected through web scraping. Organisations may rely on the PDPA's Publicly Available Exception only where the statutory conditions are met. Public availability requires more than technical accessibility: paywalls, registration requirements, access restrictions, anti-bot measures and other signals may show that the data was not intended for unrestricted collection or reuse.

The AI Guidelines also address transparency where personal data is used to train or improve a generative AI system. Generic privacy language referring only to "product improvement" may be inadequate for large-scale model training. Organisations should provide AI-specific information explaining the function of the model, the categories and use of personal data and the available mechanism to opt out or withdraw consent where applicable.

The AI Guidelines demonstrate that data sourcing and transparency must be adapted to the actual AI use case. Businesses should document why an exception or consent basis applies, respect technical and contractual access restrictions and maintain governance across model providers and deployers. Organisations operating in several jurisdictions may need different collection and notice positions rather than a single global web-scraping rule.

[14] https://files.app.optical.gov.sg/pdpc/production/assets/143cb9d4-532e-4cca-9a77-bcc0415ca294.pdf, last accessed on July 31, 2026

15 **Malaysia - Government launched Public Consultation on Proposed AI Governance Bill**[15]

Ministry of Digital, through the National AI Office, released the *Public Consultation Paper of the Proposed Artificial Intelligence (AI) Governance Bill* (**"Draft AI Governance Bill"**), that seek views on Malaysia's first broad legislative framework for the responsible development and use of AI while retaining flexibility for innovation and sector-specific implementation.

The Draft AI Governance Bill, proposes three central features: institutional oversight through a Central AI Authority, a principles-based framework built around five AI Governance Principles and a risk-based approach under which obligations would vary according to the nature and level of risk posed by an AI system. It also proposes definitions for important participants and stages in the AI lifecycle, including developers and deployers.

Two further mechanisms are under consideration in the Draft AI Governance Bill. The first is an AI incident-reporting system covering mandatory reports by developers and deployers as well as complaints from the public. The second is an AI sandbox for controlled testing before wider deployment. The Draft AI Governance Bill expressly states that it is not the complete Bill and that the Government is not bound to retain every proposal in the final legislation.

The consultation indicates that accountability is likely to extend across the AI lifecycle and attach differently to developers and deployers. Businesses operating in Malaysia should begin identifying the AI systems they use, the role they perform, the decisions affected and the process for escalating incidents. Building an AI inventory and governance record before the final law is enacted will be easier than reconstructing it once detailed obligations apply.

[15] https://upc.mpc.gov.my/view-consultation/264, last accessed on July 31, 2026

ABBREVIATIONS

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

ABBREVIATION	FULL FORM
AI	Artificial Intelligence
BCI	Bar Council of India
BNSS	Bharatiya Nagarik Suraksha Sanhita, 2023
CBDT	Central Board of Direct Taxes
CCPA	Central Consumer Protection Authority
CDSCO	Central Drug Standard Control Organization
CERT-In	Indian Computer Emergency Response
CJEU	Court of Justice of European Union
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation, 2016
NBFCs	Non-Banking Financial Companies
PDPC	Personal Data Protection Commission of Singapore
RBI	Reserve Bank of India
VDAs	Virtual Digital Assets

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

Aayush Sengupta
ASSOCIATE

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

Sagar Chaturvedi
ASSOCIATE

Supports the firm's work in technology law, data privacy, regulatory compliance and commercial advisory.

IN THE MEDIA

PERSPECTIVE

MEDIA SPOTLIGHT

Crypto reporting moved towards greater visibility

Rashmi Deshpande shared her views with The Hindu BusinessLine on the CBDT's guidance note for crypto-asset reporting and the wider move towards greater transparency and accountability in virtual digital asset transactions.

READ THE FEATURE →

FOUTAINHEAD 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.

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 is an associate and 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**.**

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.