**MONTHLY EDITION – MARCH 2026**

# TECHNOLOGY LAW

# AND

# DATA PRIVACY UPDATES

**INDEX**

**D. ABBREVIATIONS**

**E. ABOUT FOUNTAINHEAD LEGAL & CONTACT DETAILS**

**FOUNDER'S NOTE**

Welcome to this edition of Fountainhead Legal's newsletter!

This month marked a regulatory development in the form of proposed amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which seeks to strengthen intermediary compliance. The amendment proposes to make it mandatory for intermediaries to comply with any clarifications, advisories, or directions issued by the Ministry of Electronics and Information Technology. This means that Government-issued directions will now carry greater legal force, and failure to comply could affect an intermediary's safe harbour protection. This amendment raises important questions on the extent of delegated executive power.

Internationally, a landmark verdict in the US holding major social media and video-sharing platforms liable for harm arising from alleged addictive platform design marks a pivotal moment in the regulation of digital platforms. By shifting the focus from user-generated content to the behavioural design of platforms themselves, the verdict signals a growing judicial willingness to examine whether features such as algorithmic recommendations, infinite scroll, and engagement-driven interfaces create foreseeable risks of harm.

In Europe and the UK, regulators are refining data protection principles to address issues such as abusive data subject requests, age assurance obligations, and the scope of security duties. These developments indicate that legal systems are no longer reacting to technology in isolation, but are actively shaping frameworks that integrate privacy, competition, and consumer protection considerations into a unified regulatory approach.

As regulatory expectations continue to evolve, businesses that prioritise transparency, accountability, and resilience will be best positioned to navigate this dynamic environment. The law continues to evolve in response to the scale and speed of digital misuse. Complementing this, policy initiative such as the introduction of the Asset Tokenisation Bill signals an effort to facilitate innovation and investment, while maintaining regulatory oversight. Together, these developments underscore a regulatory landscape that is focused on aligning technological innovation with accountability and user protection.

We hope you find these updates insightful and informative!

## NATIONAL

### 1. Government proposes Amendment to IT Rules for Intermediaries[1]

The Government has released draft amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**"Draft Amendment"**) for public consultation. A key proposal is that directions, advisories, and guidelines issued by MeitY will become binding, and failure to comply may result in loss of safe harbour protection.

The Draft Amendment also clarifies that intermediaries must retain data even after content takedown or deletion if required under other laws, which may create overlap with data protection obligations. It further extends the Digital Media Ethics Code to user-generated news content, increasing moderation responsibilities for platforms, and expands the powers of the Inter-Departmental Committee to take up matters without a user complaint. These changes indicate higher compliance expectations and regulatory oversight for intermediaries. Comments on the Draft Amendment are to be submitted by April 14, 2026.

### 2. Delhi High Court distinguishes between Criticism and Disparagement in Media Defamation Suit[2]

Delhi High Court directed digital news platform Newslaundry Media Private Limited ("**Newslaundry**") to take down specific content identified as abusive and derogatory, and found to be disparaging TV Today Network Limited ("**TV Today**") and its channels Aaj Tak and India Today. The issue arose from a series of programmes published by Newslaundry on its digital platforms, where it critiqued and reviewed news broadcasts aired by TV Today's channels, including Aaj Tak and India Today. The order, passed on March 20, 2026, arose from cross-appeals in a defamation, copyright infringement, and commercial disparagement suit filed by TV Today in October 2021.

The court upheld the commercial disparagement. It directed the removal of abusive and derogatory characterisations of the TV Today's journalists and editorial output, from Newslaundry's website and social media platforms. The court further observed that freedom of speech, while constitutionally fundamental, does not shield communications that reflect a demonstrable intent to harm reputation rather than to engage in substantive critique, and that both parties form part of the same digital media ecosystem irrespective of their differing business models. Questions of copyright infringement and fair dealing were expressly reserved for adjudication at trial.

*This ruling draws an important interim boundary between legitimate press criticism, however pointed, and actionable commercial disparagement in the digital media segment. For content creators, journalists, and platforms whose work involves critique of competing media organisations, it signals that reliance on defences of satire and fair comment will not automatically insulate parties from injunctive relief where the language employed is prima facie derogatory and disconnected from substantive analysis.*

### 3. NHRC issues Notices over Children's Data Protection Violations[3]

The NHRC, acting on a complaint based on a research report by think tank Advanced Study Institute of Asia ("**ASIA**"), issued notices to MeitY, the Ministry of Education, and the Ministry of Communications over alleged violations of the DPDP Act by major AI, social media, and edtech

1 https://www.meity.gov.in/static/uploads/2026/03/a71a21d35c107f2e528363d3eb17646a.pdf
2 FAO(OS) (COMM) 268/2022, CM APPL. 18933/2023.
3 https://www.aninews.in/news/national/general-news/nhrc-issues-notices-over-alleged-dpdp-act-violations-by-ai-social-media-edtech-platforms20260325081218/

platforms. The ASIA report, which assessed Platforms against fourteen DPDP-based criteria, identified gaps including the absence of verifiable parental consent mechanisms, behavioural tracking and profiling of minors, and inadequate grievance redressal infrastructure. Notably, all platforms assessed impose a minimum age threshold of thirteen, creating a compliance gap with India's statutory threshold of eighteen under the DPDP Act. The NHRC directed all platforms to submit compliance reports within fifteen days and separately sought clarification on the process for issuing SIM connections to minors.

*The NHRC's intervention signals that children's data protection is transitioning from a compliance aspiration to an active enforcement under the DPDP Act and that this transition will not wait for the Data Protection Board to become fully operational. For global Platforms operating in India, the ASIA report's findings, particularly the gap between self-declared age minimums and the DPDP Act's threshold of eighteen, represent a compliance exposure that cannot be addressed through incremental policy updates alone.*

## 4. Supreme Court to examine Constitutional Validity of IT Amendment Rules on Fake Content Regulation[4]

The Supreme Court has agreed to examine the Central Government's challenge to the Bombay High Court's ruling that struck down the 2023 amendments to the IT Amendment Rules. The IT Amendment Rules had empowered the Central Government to establish a Fact Check Unit ("**FCU**") to identify content relating to Government business on social media as 'fake, false, or misleading', with intermediaries required to remove such content or display a disclaimer, failing which they risked forfeiture of safe harbour protection under Section 79 of the IT Act. The High Court struck down Rule 3(1)(v) as unconstitutional in September 2024, following a split division bench verdict finding the rule vague, over-broad, and capable of producing a chilling effect on protected expression. The Supreme Court issued notice to the original petitioners, including stand-up comedian Kunal Kamra, the Editors Guild of India, and the Association of Indian Magazines, but declined to stay the High Court's order, observing that a comprehensive final determination would be preferable.

*The Supreme Court's refusal to grant an interim stay means the FCU framework remains non-operational for now, and social media intermediaries continue to enjoy safe harbour protections without any obligation to act on Government-flagged content. The case raises foundational questions about the limits of Government-mandated fact-checking, the adequacy of procedural safeguards in content regulation, and the extent to which intermediary liability can be conditioned on compliance with executive determinations of falsity.*

## 5. Government amends Compulsory Registration Framework for Highly Specialised Electronics Equipment[5]

Government amends Paragraph 8 of the Electronics and Information Technology Goods (Requirements for Compulsory Registration) Order, 2021 to revise the exemption framework for Highly Specialised Equipment ("**HSE**").

Now, HSEs may qualify for exemption from the Compulsory Registration Scheme ("**CRS**") if it satisfies two conditions, i.e., it must either be powered by three-phase supply, or by single-phase supply with a current rating exceeding sixteen amperes, and the equipment must be manufactured or imported in fewer than one hundred units per model per year. The amendment comes into force on June 15, 2026,

[4] SLP(C) No. 6871-6873/2024.
[5] https://egazette.gov.in/WriteReadData/2026/270817.pdf?

allowing manufacturers, importers, and distributors time to review their product portfolios and ensure compliance.

*For businesses in the technology, fintech, and digital services sectors, this proposal warrants close monitoring, particularly as it develops alongside India's broader data governance framework under the DPDP Act and the Government's simultaneous push to deepen digital adoption.*

## 6. Delhi High Court protects Personality Rights through Dynamic+ Injunction

Building on the trend of dynamic injunctions, courts have further refined their anti-piracy by issuing dynamic plus injunctions that offer ex-ante protection, covering content that has not yet been publicly released at the time the order is made. Earlier this year, the Delhi High Court strengthened protections[6] for global entertainment companies by directing the blocking of websites illegally hosting pirated films and television series.

Separately, on a plea filed by the UEFA, again the court directed[7] internet service providers and domain name registrars to restrict access to pirate platforms during the UEFA's Champions League 2025-26 season. Unlike John Doe blocking orders which require rights holders to approach the court for each new infringing URL, dynamic plus injunctions empower plaintiffs to add mirror sites and alphanumeric pirate domains directly through the court's administrative office, without the need to seek a fresh hearing on each occasion.

*The evolution from static URL-based orders to dynamic plus injunctions reflects judicial recognition of the asymmetry between rights holders and piracy networks that reconstitute themselves almost instantly under new domain names, mirror sites, and encrypted platforms. For rights holders and content platforms, this jurisprudential shift strengthens the practical value of injunctive relief in the digital environment.*

## 7. Bill to Regulate Asset Tokenization introduced in Parliament[8]

The Asset Tokenisation (Regulation) Bill, 2026 (**"Bill"**) has been introduced in Rajya Sabha as a Private Member's Bill on March 14, 2026, marking India's first dedicated legislative proposal for regulating tokenised real-world assets. The Bill seeks to provide legal recognition to asset tokenisation and establish a statutory framework for the issuance, trading, custody, and settlement of tokenised assets representing real-world holdings, including a pathway for regulating stablecoins. The Bill proposes a multi-regulatory oversight model aligned with international standards, with regulatory responsibilities distributed across existing financial sector regulators. The Bill aims to bring legal clarity, transparency, and investor protection to an ecosystem that, despite significant growth in blockchain adoption, has operated without a formal regulatory framework in India.

*The Bill signals a move toward formal recognition of tokenised real-world assets in India, providing much-needed clarity for emerging trends such as fractional ownership and digital securities. However, the proposed multi-regulator approach may also increase compliance complexity, suggesting that regulatory acceptance will be accompanied by more structured oversight.*

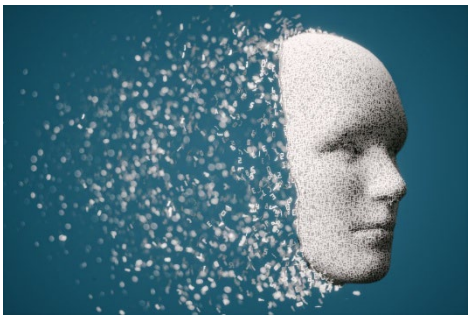
[6] CS(COMM) 250/2020 and I.A. 2285/2024
[7] CS(COMM) No. 106 of 2026
[8] https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/18e3192026103415AM.pdf?source=legislation

## INTERNATIONAL

## UNITED STATES OF AMERICA

### 8. Court blocks Government's Action against AI Company Over Safety Restrictions[9]

AI company Anthropic PBC ("**Company**") filed suit before the US District Court for the Northern District of California challenging its classification as a 'national security supply-chain risk' by Department of Defence. The dispute arose after the Company refused to remove two safeguards from its 'Claude' model usage policy. This included a prohibition on use in fully autonomous lethal weapons systems, and a prohibition on domestic mass surveillance of citizens. Following this refusal, the Defence Secretary classified the Company as a 'supply-chain risk' and the President directed all federal agencies to cease use of its technology, with a six-month phase-out period. On March 26, 2026, the court granted a preliminary injunction in the Company's' favour, finding that the Government's actions appeared to be directed at punishing the Company for its publicly stated AI safety positions, rather than any legitimate national security concern, conduct the court characterised as textbook First Amendment retaliation. The Company separately filed a second suit in Washington D.C. challenging a related designation that could affect its eligibility for civilian Government contracts.



*The case highlights a growing tension between AI safety commitments and public-sector expectations, particularly where technology providers seek to restrict high-risk uses of their systems. For businesses, it underscores the importance of clearly defining permissible use cases upfront and anticipating potential conflicts between ethical safeguards, contractual obligations, and Government requirements.*

### 9. AI Research Company sued for IP Infringement over AI Training[10]

Encyclopaedia Britannica, Inc. (**"Britannica"**) and its subsidiary Merriam-Webster Inc. (collectively **"Plaintiffs"**) filed suit on March 13, 2026, in the US District Court for the Southern District of New York against OpenAI Inc. ("**OpenAI**"), alleging large-scale copyright infringement and trademark violation. The complaint alleges that OpenAI unlawfully scraped and used nearly one hundred thousand of Britannica's online articles and dictionary definitions to train its GPT family of large language models without permission, and that ChatGPT generates outputs that reproduce or closely paraphrase this protected content, diverting users who would otherwise visit the Plaintiffs' own platforms.

The Plaintiffs further allege trademark infringement, contending that ChatGPT's hallucinations falsely attribute fabricated content to Britannica, creating a misleading impression of authorisation. OpenAI has disputed the claims, contending that its models were trained on publicly available material and that such use falls within the fair use doctrine. The filing marks the second major copyright action brought by the same plaintiffs, having previously sued AI search engine Perplexity on substantially similar grounds in September 2025.

*The case reflects a broader global debate on the use of copyrighted material for training AI models, an issue that is also being tested in India in the ANI vs. OpenAI litigation. Both matters raise similar questions around training data consent, fair use, output reproduction, and attribution, particularly where AI-generated responses may substitute original sources. For AI developers and platforms operating in India, these developments signal that questions around data sourcing, licensing, and output accountability are likely to come under closer judicial and regulatory scrutiny in the near term.*

---

[9] Anthropic PBC v. U.S. Department of War, 3:26-cv-01996, (N.D. Cal.)

[10] Encycolpedia Britannica Inc. and Merriam-Webster Inc., v. OpenAI, Inc., Civil Action No. 1:26-cv-2097

## 10. Healthcare Records Company sues Health Information Network alleging fraudulent Patient Data Access[11]

Epic Systems Corporation ("**Epic**"), the dominant provider of electronic health record systems, filed a federal lawsuit in the US District Court for the Central District of California, alongside a group of healthcare providers. The suit alleges that Health Gorilla Inc., a health information network, enabled at least two companies, Mammoth Path Solution LLC and RavillaMed PLLC, to fraudulently access and commercially exploit the medical records of approximately three hundred thousand patients from Epic's network, as well as records from the Department of Veterans Affairs and other providers. The defendants allegedly presented themselves as healthcare providers seeking records for treatment purposes, while in fact aggregating and reselling sensitive patient data, including genetic, mental health, and reproductive information, to law firms seeking mass tort claimants. The scheme allegedly relied on fictitious websites, shell entities, and fraudulent National Provider Identification ("**NPI**") numbers to disguise the true purpose of data access. One defendant, GuardDog Telehealth, subsequently admitted to improper access and agreed to be barred from health information exchanges.

*The case highlights the risks that arise when trust-based access systems are exploited at scale, particularly in health information networks where data is highly sensitive. As digital health ecosystems expand, including in India under initiatives like Ayushman Bharat Digital Mission, the focus must shift from enabling access to verifying legitimacy at every stage of data use. For businesses operating in this space, this underscores the need for robust onboarding checks, strict purpose-limitation controls, and continuous monitoring of access patterns. Without these safeguards, systems designed to improve healthcare delivery can be misused for large-scale data aggregation and commercial exploitation.*

## 11. Oklahoma enacts Comprehensive Consumer Data Privacy Law[12]

Oklahoma Governor Kevin Stitt signed Senate Bill 546 ("**OCDPA**") a comprehensive consumer data privacy law, effective from January 1, 2027. The OCDPA applies to controllers and processors conducting business in Oklahoma or targeting Oklahoma residents, who either process the personal data of at least one hundred thousand consumers annually, or process data of at least twenty-five thousand consumers while deriving more than fifty per cent of gross revenue from data sales.

Modelled on the Virginia consumer privacy framework, OCDPA grants Oklahoma consumers rights of access, correction, deletion, portability, and opt-out from targeted advertising, data sales, and certain profiling activities. Controllers are required to publish clear privacy notices, conduct data protection assessments for high-risk processing activities, and obtain explicit consent for the processing of sensitive personal data. Enforcement rests solely with the Oklahoma Attorney General, who must provide a thirty-day right to cure before initiating action, with civil penalties of up to USD 7,500 per violation.

*For organisations already compliant with other state privacy laws, the practical priority will be ensuring that data protection assessments, consent workflows, and privacy notices are appropriately configured for Oklahoma residents well in advance of the January 2027 effective date.*

[11] Epic Systems Corporation v. Health Gorilla, Inc., 2:26-cv-00321, (C.D. Cal.).
[12] https://www.okhouse.gov/posts/news-20260323_2.

## 12. Major Tech Platform rolls back Direct Message privacy feature[13]

Meta Platforms Inc. ("**Meta**") announced that end-to-end encryption ("**E2EE**") for Instagram direct messages will cease to be available after May 8, 2026, effectively reversing a privacy feature introduced on an opt-in basis in 2021. Meta attributed the decision to low user uptake, directing users wishing to retain E2EE messaging to migrate to WhatsApp Inc. From May 8, 2026, Instagram direct messages will be accessible to Meta at the infrastructure level, reopening the platform to automated content moderation, AI-driven scam detection, and compliance with law enforcement requests. The announcement is notable in its timing with the Take It Down Act, 2025 requiring platforms to remove certain content within forty-eight hours of a removal notice, takes effect on May 19, 2026, and E2EE significantly complicates compliance with such obligations. Meta's decision coincides with the European Parliament's extension of a temporary exemption permitting voluntary detection of child sexual abuse material until August 2027.

*For users, and in particular for journalists, activists, and professionals who relied on the feature for confidential communications, the practical consequence is that direct message content becomes accessible to Meta for moderation, advertising personalisation, and legal requests. For digital platforms globally, this development reinforces the importance of clearly disclosing to users the actual privacy protections applicable to their communications.*

## 13. SEC and CFTC issue landmark Joint Interpretation on Crypto Asset Classification[14]

Securities and Exchange Commission ("**SEC**") and the Commodity Futures Trading Commission ("**CFTC**") jointly issued a comprehensive interpretive release (**"Release"**) clarifying the application of federal securities laws to crypto assets and transactions, the most definitive regulatory statement on digital assets in over a decade. The interpretation establishes a five-part token taxonomy, categorising crypto assets as digital commodities, digital collectibles, digital tools, payment stablecoins, or digital securities, with only the last category remaining subject to full securities regulation.

The Release addresses the circumstances under which a non-security crypto asset may become subject to an investment contract based on issuer representations, and equally, when such obligations cease upon sufficient network decentralisation. The Release also addresses specific activities including airdrops, protocol mining, staking, and the wrapping of non-security assets, and expressly supersedes prior SEC staff guidance including the 2019 digital assets framework. The Release follows a memorandum of understanding signed between the SEC and CFTC on March 11, 2026.

*The joint interpretation reflects a more structured and coordinated approach to classifying and regulating crypto assets, moving away from fragmented enforcement-driven guidance. For India, this is particularly relevant in light of the proposed Asset Tokenisation (Regulation) Bill, 2026, which similarly seeks to bring clarity to tokenised assets through a defined regulatory framework. Together, these developments indicate a broader global shift toward categorisation-based regulation of digital assets, where legal treatment depends on the nature and function of the asset rather than a one-size-fits-all approach.*

[13] https://help.instagram.com/491565145294150
[14] https://www.sec.gov/files/rules/interp/2026/33-11412.pdf .

**EUROPEAN UNION**

## 14. CJEU permits refusal of GDPR Access Requests driven by Compensation Motives[15]

CJEU delivered its judgment in Brillen Rottler (Case C-526/24) on March 19, 2026, clarifying that a data subject's request for access to personal data under Article 15 of the GDPR may, in certain circumstances, be refused as excessive where it is made not for the purpose of verifying lawful processing, but with the abusive intention of artificially creating conditions for a compensation claim under Article 82 of the GDPR.

The issue arose from an individual who subscribed to an optician's newsletter, lodged a data subject access request merely thirteen days later, and subsequently sought at least GBP 1,000 in compensation upon the request being refused. The CJEU held that evidence of a data subject having systematically submitted access requests across multiple controllers followed by compensation claims may be taken into account in establishing such abusive intent. The CJEU further clarified that compensation under GDPR requires the actual demonstration of damage, and that where the data subject's own conduct is the determining cause of the alleged harm, compensation may be denied.

*This judgment gives data controllers a meaningful tool to push back against industrialised DSARs-for-compensation schemes. By confirming that even a first request can be deemed excessive where bad faith is demonstrable, the CJEU offers practical relief from systematic rights abuse. Organisations should nonetheless ensure refusals are well-evidenced and documented, as the burden of establishing abusive intent rests with the controller.*

[15] https://curia.europa.eu/site/upload/docs/application/pdf/2026-03/cp260038en.pdf

**UNITED KINGDOM**

## 15. ICO and Ofcom issue Joint Statement on Age Assurance Obligations[16]

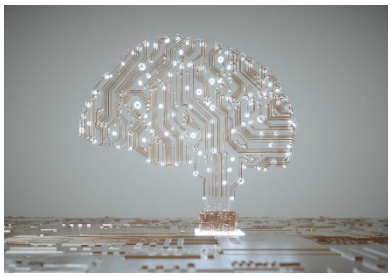
The Digital Regulation Cooperation Forum published a joint policy statement (**"Statement"**) by the Information Commissioner's Office ("**ICO**") and the Office of Communications ("**Ofcom**"), setting out how online services can simultaneously discharge age verification obligations and protect users' personal information.

The Statement addresses how organisations implementing age assurance tools can adopt a risk-based, privacy-compliant approach, and confirms that organisations should consult both Ofcom's online safety guidance and the ICO's data protection guidance to ensure that their chosen age assurance processes satisfy both online safety and data protection obligations concurrently. The Statement aims to provide clarity on the selection and deployment of age assurance mechanisms that are proportionate, privacy-preserving, and consistent with applicable regulatory expectations under both the UK Online Safety Act 2023 and the UK General Data Protection Regulation 2016.

*The takeaway for organisations is that age assurance cannot be implemented as a purely technical compliance exercise, it must be designed with data minimisation, purpose limitation, and proportionality embedded from the outset. For platforms with a UK user base, or for those assessing how to address comparable age-gating requirements as they emerge in other jurisdictions, this joint regulatory approach offers a useful and adaptable model.*

## 16. Court of Appeal confirms Data Security Obligations extend to Pseudonymised Data[17]

The Court of Appeal (**"Court"**) handed down its judgment in DSG Retail Limited v. The Information Commissioner[18] confirming that a data controller's duty to implement appropriate security measures applies to all personal data it processes irrespective of whether a third-party attacker who exfiltrates that data would be capable of identifying the individuals concerned. The case arose from a large-scale cyberattack on Dixons Stores Group Retail Limited (operators of Dixons and Currys PC World) ("**DSG**") between 2017 and 2018, during which transaction data from over 5.6 million payment cards was compromised, including card numbers and expiry dates but not, in most instances, directly identifying information. DSG contended that since attackers could not re-identify individuals from the stolen data, no personal data breach had occurred. The court rejected this reasoning, holding that the identifiability test for the purposes of the security obligation must be assessed from the controller's own perspective, not the attackers. The court confirmed that truly anonymised data, from which no individual can be identified even by the controller, falls outside the security duty, preserving the legally significant distinction between pseudonymisation and genuine anonymisation.



*For data protection officers and information security teams, this reinforces the need to apply robust technical and organisational measures across the full breadth of personal data processed, and to resist the temptation to calibrate security investment by reference to the re-identification capabilities of a hypothetical external actor.*

---

[16] https://ico.org.uk/media2/5ybpmabf/ofcom-ico-joint-statement.pdf

[17] https://www.judiciary.uk/wp-content/uploads/2026/02/ICO-v-DSG-2026-EWCA-Civ-140-FINAL-for-hand-down.pdf

[18] [2026] EWCA Civ 140

## 17. ICO issues Guidance on new 'Recognised Legitimate Interests' Lawful Basis[19]

The Information Commissioner's Office ("**ICO**") published guidance on March 23, 2026, clarifying the operation of the new 'recognised legitimate interests' ("**RLI**") lawful basis introduced into the UK GDPR by the Data (Use and Access) Act 2025 ("**DUAA**"), which came into force on February 5, 2026. The RLI basis constitutes a seventh lawful ground for processing personal data and differs materially from the existing legitimate interest's basis in that it does not require controllers to conduct a balancing test weighing organisational interests against data subject rights.

Five pre-approved qualifying purposes are specified: national security, public security, and defence; detection, investigation, or prevention of crime; responding to requests from public interest bodies; responding to emergency situations; and safeguarding vulnerable individuals. Controllers must still assess necessity, comply with all other data protection obligations, maintain transparency with data subjects, and update their records of processing activities and privacy notices accordingly. The RLI basis is unavailable to public authorities, cannot underpin significant automated decision-making, and does not extend to routine commercial processing such as direct marketing or intra-group data transfers.

*For data protection officers and privacy teams, the immediate priorities are updating records of processing activities and privacy notices to reflect the new basis, and auditing existing processing activities to assess whether any currently justified under general legitimate interests could more appropriately migrate to RLI.*

**SWITZERLAND**

## 18. Federal Data Protection Commissioner issues Consumer Guide on Wearable Device Privacy[20]

Federal Data Protection and Information Commissioner ("**FDPIC**") published a consumer-facing guidance document on the data protection implications of wearable devices, covering smartwatches, fitness trackers, and smart glasses. The guidance explains the privacy risks arising from the continuous collection of sensitive personal data, including sleep patterns, cardiac data, geolocation, and audio and image information, by body-worn internet-connected devices, noting that such data collection may also affect third parties in the vicinity of the wearer. The FDPIC advises consumers to assess, before purchase, whether a manufacturer has configured privacy-friendly default settings, the geographic location of data storage, and whether processing practices are transparent and comprehensible. The guide devotes particular attention to smart glasses, highlighting the heightened sensitivity arising from their capacity to passively capture third parties without notice or consent, a concern that grows more acute as commercially available AI-integrated eyewear proliferates.

*For businesses developing or deploying wearable technology targeting Swiss consumers, this guidance underscores the importance of privacy-by-design product architectures, transparent data processing disclosures, and default settings that minimise collection not merely as compliance obligations, but as a baseline expectation of consumer trust.*

[19] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/recognised-legitimate-interest/

[20] https://www.edoeb.admin.ch/fr/objets-connectes-ce-quil-faut-savoir-pour-bien-les-acheter-et-sen-servir

**ABBREVIATIONS**

**AI –** Artificial Intelligence

**CJEU –** Chief Justice of European Union

**DPDP Act –** Digital Personal Data Protection Act, 2023

**DPIIT –** Department for Promotion of Industry and Internal Trade

**EU –** European Union

**EWCA Civ –** England and Wales Court of Appeal (Civil Division)

**FDI –** Foreign Direct Investment

**GDPR –** General Data Protection Regulation, 2016

**GPT –** Generative Pre-trained Transformer

**Inc. / Ltd. / PBC –** Incorporated / Limited / Public Benefit Corporation

**IT Rules –** Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

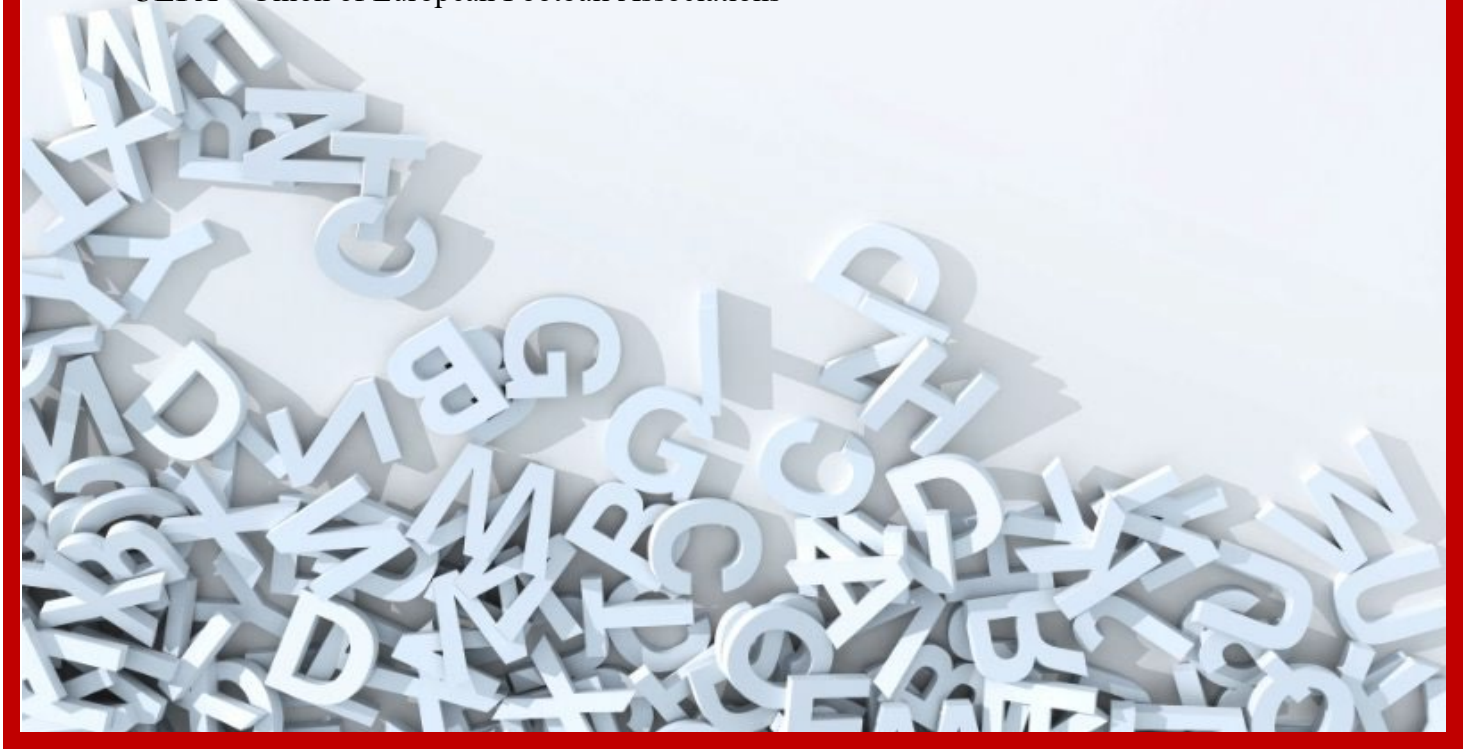
**ITES –** Information Technology Enabled Services

**MeitY** – Ministry of Electronics and Information Technology

**NHRC** – National Human Rights Commission

**SIM –** Subscriber Identity Module

**UEFA** – Union of European Football Associations



## ABOUT FOUNTAINHEAD LEGAL

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

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

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

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

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

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

**CONTACT DETAILS**

**Rashmi Deshpande**

Email: rashmi@fountainheadlegal.com

Contact Number: +91 98338 62234

LinkedIn: https://www.linkedin.com/in/rashmi-deshpande-3775b336/

**Aarushi Ghai**

Email: aarushi@fountainheadlegal.com

Contact Number: +91 91314 15290

LinkedIn: https://www.linkedin.com/in/aarushi-ghai-282130179/

**Vaibhav Gupta**

Email: vaibhav@fountainheadlegal.com

Contact Number: +91 77987 96778

LinkedIn: https://www.linkedin.com/in/vaibhavguptav21/

**Address**

C - 2106, Oberoi Garden Estate,

Chandivali Farm Road, Powai – 400 072

**Website**: https://fountainheadlegal.com/

**LinkedIn**: https://www.linkedin.com/company/fountainhead-legal/