

THE PRIVY TIMES

The Processors' Dilemma: Why it's time for sectoral regulators to step in

P4

Expert opinions: Unpacking the DPDP Rules

P8

What's missing in the DPDP draft rules?

P9

Avoid

₹250 Cr

Fine

Gain customer trust

Stop spamming me!! 🤯

👁️ Who gave you my data!!

Get DPDPA Compliant

#PrivacyMatters

Scan to join our DPO
WhatsApp Group



Big Tech algorithms will need to prioritize Data Localization for certain data types



The Indian government has unveiled significant new requirements for major technology companies through the DPDP draft rules. Released on January 3, 2025, these rules introduce two major obligations for companies designated as "significant data fiduciaries."

First, these companies must verify that their algorithms for processing personal data pose no risk to user rights. These rights encompass access to information, data erasure, objection, and redress. This requirement shifts algorithmic oversight from the proposed Digital India Bill to the DPDP framework.

Second, the rules establish data localization requirements. Companies must process and store certain government-specified personal data exclusively within India's borders. A designated committee will recommend which types of personal data fall under these restrictions, preventing their transfer outside Indian territory.

The government will classify organizations as significant data fiduciaries based on several factors: the volume of personal data they process, potential risks to users and democratic processes, and their overall impact. This designation will likely apply to major multinational corporations and tech platforms operating in India.

Additional obligations for these entities include:

- Conducting and reporting data protection impact assessments
- Submitting to regular audits
- Providing detailed reports to the Data Protection Board

These draft rules, open for public feedback until February 18, represent a substantial evolution in India's approach to data governance. They particularly focus on protecting user rights while establishing clearer oversight of algorithmic systems and data flows.

India's DPDP draft rules mandate user data deletion after 3 years for ecom, social media companies

India's new data protection regulations under the DPDP Act have introduced significant requirements for major digital platforms. According to the draft rules released for public consultation, large-scale digital businesses must implement strict data deletion policies.

The regulations specifically target three categories of digital platforms with substantial user bases in India: e-commerce companies with over 20 million registered users, gaming platforms with more than 5 million users, and social media platforms exceeding 20 million users. These entities must remove users' personal information three

years after it is no longer necessary for its original purpose.

However, the rules require platforms to notify users 48 hours before data deletion, giving individuals the opportunity to request data retention if needed for accessing services. The rules also outline comprehensive breach notification requirements, mandating that companies inform affected users promptly about any data breaches, including details about the incident's nature, potential impacts, and remedial measures.

The rules particularly focus on cross-border data transfers, suggesting potential additional oversight through a committee that may recommend restrictions



on certain types of personal data being transferred outside India. This adds a new layer of complexity to international data handling practices.

These draft rules, open for public feedback until February 18, 2025, represent a significant

evolution in India's approach to data privacy. They aim to balance user protection with practical business operations, though some stakeholders note that certain scenarios and use cases still need to be addressed in the final version.

Startup leaders voice concerns around DPDP A, government promises separate dialogue

During a consultation on January 16, 2025, startup founders raised significant concerns about India's DPDP draft rules during discussions with government officials. The Ministry of Electronics and Information Technology (MeitY) Secretary S. Krishnan led the session, which included representatives from prominent startups such as Razorpay, Khatabook, and Dream 11.

Key concerns centered on cross-border data transfer restrictions for significant data fiduciaries

(SDFs) and the implementation of consent manager roles. Several founders emphasized the necessity of international data transfers for specific industries like e-commerce and travel. In response, government officials indicated potential caveats would be added to the rules.

The startup community also highlighted challenges regarding regulatory overlap, particularly for sectors already governed by specific regulations. Fintech and insurance companies, for instance, must navigate existing RBI and IRDAI guidelines alongside the

new DPDP requirements.

Questions emerged about consent manager specifications, including whether these intermediaries should be independent third parties or data fiduciaries themselves. The rules require consent managers to maintain a minimum net worth of Rs 2 crore and meet specific technical criteria.

MeitY minister, Ashwini Vaishnaw's recent public consultation suggested a possible extension of the feedback submission deadline beyond February 18. The government

emphasized on balancing innovation with regulation, promising focused consultations with various stakeholders.

International business groups, particularly the US-India Business Council, warn that ambiguity in data transfer restrictions could impact foreign investment in India. The government's response to these concerns and its commitment to separate startup consultations indicates a willingness to refine the rules while maintaining their core protective framework.



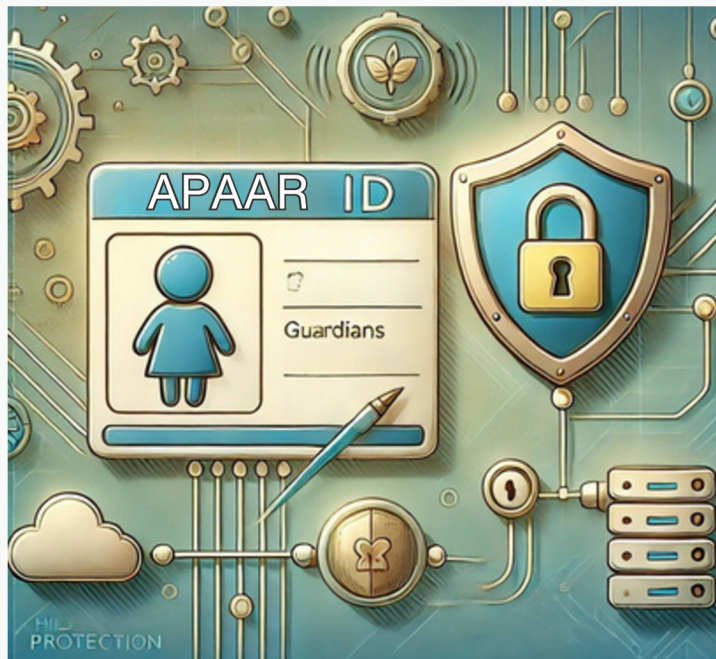
APAAR IDs may be used to verify guardians for processing children's data

If you're a parent, you may have already had a request from your kid's school to create their APAAR ID.

India's draft Digital Personal Data Protection (DPDP) Rules propose using emerging digital identification systems to verify parental consent for processing children's data. The framework suggests incorporating the Automated Permanent Academic Account Registry (APAAR) ID, a national student identification system, and state-level family IDs for guardian verification.

While no national family ID system exists currently, several states including Haryana, Andhra Pradesh, Tamil Nadu, and Rajasthan have implemented local family identification frameworks. These systems could be integrated into the parental consent verification process under the new rules.

The draft mandates data fiduciaries to implement technical measures for verifying parent or guardian identity through government-issued IDs or digital tokens linked to trusted services. MeitY minister, Ashwini Vaishnaw emphasized that virtual tokens used for children's data



verification will be temporary and self-destructing after single use. The proposal addresses privacy concerns through mandatory security safeguards and oversight by consent managers. However, questions remain about data interoperability between different state-level systems and privacy protection mechanisms.

The rules are part of broader efforts to protect children's digital privacy while ensuring they can

benefit from technology safely. The government has opened these draft rules for public consultation until February 18, 2025, indicating willingness to refine the framework based on stakeholder feedback.

This initiative aligns with India's "One Nation, One Student ID" program, demonstrating a shift toward integrated digital governance while prioritizing data protection for minors.

FTC updates children's privacy law by including biometric data protection



Across the seas in the US, the Federal Trade Commission has finalized significant updates to the Children's Online Privacy Protection Act (COPPA), expanding protections to include biometric data and government IDs. The unanimous decision requires companies to obtain explicit parental consent before sharing children's data with third parties for advertising.

Key changes include strict data retention limits and broader definitions of personal information covering facial recognition and fingerprint data. Companies must now delete children's data once it's no longer

necessary for its original purpose. The rule strengthens transparency requirements for 'Safe Harbor' programs, mandating public membership lists and additional reporting. While some proposed changes, like push notification restrictions, weren't adopted, companies have one year to comply with the new requirements.

Commissioner Ferguson, Trump's FTC pick, criticized the timing of these changes and raised concerns about compliance costs and potential market impacts. However, FTC Chair, Lina Khan emphasized the importance of preventing unauthorized monetization of children's data in the digital age.

Australia's bold move: Social media ban for under-16s sets global precedent

Australia has enacted a landmark legislation banning social media access for children under 16, becoming the first nation to implement such comprehensive restrictions. The law, set to take effect in late 2025, will require platforms like Instagram, Facebook, and TikTok to prevent minors from creating accounts or face penalties up to A\$49.5 million (\$32 million).

The legislation emerged from growing concerns about social media's impact on youth mental health, backed by 77% of Australians according to recent polls. While YouTube remains exempt due to its educational use, major platforms must participate

in age verification trials starting January 2025.

The ban has sparked divided reactions. Parent groups and anti-bullying advocates support the measure, citing the U.S. Surgeon General's warnings about social media's role in youth mental health issues. However, critics, including human rights organizations and youth advocacy groups, warn it could isolate vulnerable teens from support networks.

Tech companies have expressed concerns about implementation challenges. Meta highlighted the need for "technically feasible" solutions that won't burden parents and teens, while industry

groups question proceeding with the ban before age verification trials conclude.

The law marks another chapter in Australia's assertive regulation of tech giants, following earlier legislation requiring platforms to pay media outlets for content sharing. It also sets a precedent for other jurisdictions considering similar restrictions, though differing from partial bans in France and some U.S. states that allow parental consent.

The legislation includes privacy safeguards, requiring platforms to offer alternatives to ID document uploads for verification. A 12-month implementation period will allow consultation between tech

companies and regulators to develop practical compliance methods.



Making the transition from contracts to continuous processor compliance

How do you as a fiduciary manage your processors in the age of the DPDP Act?

The DPDP Act has shifted the balance of accountability for data protection in India. Fiduciaries—organizations that determine the purpose and means of data processing—now bear full responsibility for their processors' actions. Unlike processors, who face no direct penalties under the law, fiduciaries are liable for every misstep, making it imperative for them to rethink how they manage their vendors. Until now, vendor management in India often relied heavily on paperwork. Contracts were drafted, signed, and filed away, with little active monitoring of compliance. But the DPDP Act has made one thing clear: a contract alone won't save you. Fiduciaries must move beyond the legal comfort of agreements



and ensure real-world compliance through proactive oversight.

Consider this scenario: a data principal withdraws their consent for personal data. The DPDP Act requires fiduciaries not only to erase the data they hold but also to ensure that any

processors acting on their behalf do the same. This dual responsibility means that fiduciaries must actively track their processors' compliance, ensuring data deletion is carried out promptly and systematically. For instance, if a fiduciary routes 10,000 data deletion requests to a processor, yet only 6,000 are

fulfilled, the fiduciary is liable for addressing the gap. This cannot be handled passively or on a case-by-case basis, and robust systems are needed to periodically monitor processors' adherence, flag inconsistencies, and enforce consequences where necessary.

This new reality is set to transform vendor onboarding. Businesses can no longer onboard processors based solely on costs or timelines. Due diligence, ongoing monitoring, and clearly defining contractual obligations are now non-negotiable. The days of passive vendor relationships are over. DPOs will play a crucial role in this shift, as they step into positions of operational authority, ensuring that processors don't just promise compliance but demonstrate it.

The Cookie PII that nobody noticed



Every time you browse the internet, tiny pieces of code called cookies latch onto your browser. They promise convenience—remembering your logins, saving your shopping cart, or showing you relevant content.

At first glance, cookies may seem harmless. They don't directly store your name, email, or phone number—so why are they a privacy concern? The truth lies in what they indirectly reveal. Cookies track everything from your browsing habits and preferences to device details like your IP address. Over time, this data is stitched together to form a detailed digital profile of you, which can often lead to indirect identification, making it personal data. Consider another example: you visit a fitness website to browse treadmills. A third-party cookie records your activity and matches it to your IP address. Days later, while reading the news, you're bombarded with ads for the same treadmill. Over time, these cookies observe patterns—your browsing times, your location, even the devices connected to your home Wi-Fi. Without directly storing your name, the cookie remembers your device and builds a profile that's eerily personal.

Worse, such tracking can lead to discriminatory outcomes. Your interest in luxury items could result in higher airfare quotes, while your browsing of health-related sites might make insurers cautious. While the DPDP Act doesn't explicitly mention cookies, they clearly fall under its broad definition of personal data due to their ability to indirectly identify individuals. As India's data protection laws evolve, it remains to be seen whether fiduciaries will treat cookies as part of personally data or if further clarification is needed.

The Processors' Dilemma: Why it's time for sectoral regulators to step in

In India's rapidly evolving digital landscape, particularly in sectors like insurance, lending, and banking, there are certain complex data processing journeys that require the attention of sectoral regulators. While the DPDP Act provides clear guidelines on responsibilities for personal data, these intricate digital processes demand further clarity from regulators to ensure compliance and accountability across industries.

Take insurance web aggregators like Policybazaar and PhonePe, which work with insurance providers such as Max Life or LIC. These aggregators collect user data to help people purchase insurance products, while the insurance providers handle essential tasks like verifying health histories and identities. Here's the question: Should aggregators collect consent for both their processing activities (like marketing and account setup) and the insurers' activities (such as health verification)? Or should each entity—aggregators and insurers—seek separate consent for their respective roles?

This situation could lead to consent fatigue, where users are bombarded with multiple consent notices, potentially

making it difficult for them to understand who is processing their data and for what purpose. If the consent process is handled by both the aggregators and insurers, should they be treated as joint fiduciaries, each with shared responsibility for the data? Or is the aggregator merely a processor, acting on behalf of the insurer?

Similar issues arise in the world of co-branded credit cards, where both the bank and its partner (for instance, an airline) determine how customer data will be processed. Who is responsible for showing the consent notice in these cases? Can the partner (the processor) seek consent on behalf of the bank (the fiduciary)? Another example comes from the rapidly expanding Digital Lending Apps (DLAs), that often partner with multiple banks and NBFCs. These DLAs collect user data and share it with their banking partners. Are the banks acting as fiduciaries, or are they simply processors in this context? If the DLA is seeking consent, is it doing so on behalf of all the banks and NBFCs with whom it shares data? The legal and operational implications are even more complex. For example, when a loan is disbursed, should all the

financial institutions with whom the data was shared delete the user's personal information? And should the banks and NBFCs retain the data, or are they required to delete it once the loan is processed?

To clarify these responsibilities, sectoral regulators like RBI, IRDAI, and SEBI will need to step in and provide clear guidelines. They will play a vital role in defining who is responsible for collecting consent, processing data, and managing data retention across

multiple entities. This will help ensure that the data protection ecosystem remains robust, with clear responsibilities for each player, whether they are acting as a fiduciary, a processor, or a joint fiduciary.

The future of data protection in India will depend on how regulators address these emerging complexities and whether businesses can adapt to a new standard for data management that prioritizes user consent and transparency.



Change Healthcare Ransomware Breach

IMPACT:
Largest healthcare data breach to date, affecting 100 million individuals (54% of the year's breached records).

CAUSE:
Lack of multifactor authentication on a Citrix portal led to unauthorized access.

OUTCOME:
A \$22 million ransom paid to BlackCat/ALPHV ransomware group; the data was still leaked.

CONSEQUENCES:
Severe operational disruptions, patient care challenges, and scrutiny of healthcare consolidation and cybersecurity practices.

Kaiser Foundation Health Plan Pixel Breach

IMPACT:
Up to 13.4 million individuals' data exposed due to third-party tracking tools.

CAUSE:
Use of tracking pixels

DETAILS:
These tools shared sensitive user interactions with third parties (Meta, Google, etc.), potentially revealing private health information.

REGULATORY RESPONSE:
The breach occurred amidst conflicting rulings on HIPAA compliance for tracking tools, with updated guidance limiting their use to unauthenticated web pages.



Ascension Health Ransomware Attack

IMPACT:
Affected the protected health information of 5.5 million patients and caused a month-long electronic health record outage.

CAUSE:
Initial access through a malicious file downloaded by an employee.

OUTCOME:
Operational disruptions across 142 hospitals, with delayed notifications to affected individuals, raising concerns about response preparedness.



BSNL Data Breach



IMPACT:
Exposed critical telecom data, including IMSI numbers and SIM details.

CAUSE:
A server compromise identified by CERT-In.

OUTCOME:
No service disruptions but heightened risks of SIM cloning and unauthorized network access. Prompted government action to audit telecom security.

Meta Fined Over WhatsApp Privacy Practices

FINE:
₹213.14 crore penalty by the Competition Commission of India.

ISSUE:
Mandatory data sharing with Meta companies without opt-out options.

OUTCOME:
A five-year ban on sharing WhatsApp data with Meta for advertising, mandatory transparency measures, and user autonomy improvements.



OpenAI Fined for ChatGPT Privacy Violations



FINE:
€15 million penalty from Italy's data protection authority.

ISSUES:
Lack of legal basis for data use, inadequate transparency, and insufficient age verification.

OUTCOME:
Mandated public education on data practices and heightened scrutiny of AI privacy compliance.

Netflix's GDPR Violation

FINE:
€4.75 million by the Dutch Data Protection Authority.

ISSUES:
Failure to provide clear information on data usage, retention, and third-party sharing.

OUTCOME:
Netflix updated its privacy policy and is appealing the fine, highlighting ongoing regulatory pressure in the EU.



Apple Siri Privacy Breach

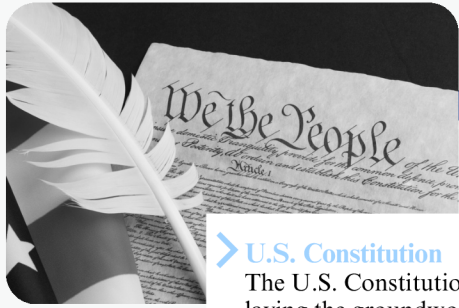


SETTLEMENT:
\$95 million to resolve allegations of accidental recording of private conversations by Siri.

DETAILS:
Recordings captured sensitive information unintentionally and reviewed by contractors for quality control.

OUTCOME:
Eligible U.S. users may receive compensation, but questions remain about the adequacy of the settlement as a deterrent.

These incidents illustrate the critical importance of robust cybersecurity practices, regulatory compliance, and transparency in handling sensitive data. They also underline the challenges posed by technology missteps and the growing scrutiny from governments and watchdogs worldwide.



1789

> U.S. Constitution

The U.S. Constitution came into effect, laying the groundwork for the legal framework of the United States. While it doesn't explicitly mention a right to privacy, the Supreme Court has interpreted certain amendments—such as the First, Third, Fourth, and Fifth—as providing protections related to privacy.

1890

> The "Right to Privacy" Article

Louis Brandeis and Samuel Warren authored an article titled *The Right to Privacy*, published in the *Harvard Law Review*. This pivotal piece argued for the recognition of privacy as a legal right, citing the growing impact of photography and the press on personal lives.

1914

> Creation of the Federal Trade Commission (FTC)

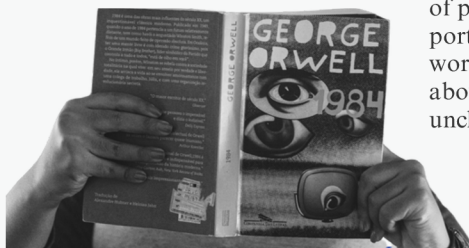
The Federal Trade Commission Act established the FTC to combat unfair or deceptive practices in commerce. By the 1970s, the FTC emerged as a key player in addressing privacy concerns and enforcing regulations.



1948

> 1984 by George Orwell

George Orwell's 1984 depicted a dystopian society with pervasive surveillance and loss of privacy. The novel's portrayal of a state-controlled world remains a stark warning about the dangers of unchecked oversight.



1917

> Defense of Sealed Mail

During World War I, the U.S. government sought to expand surveillance efforts. Judge William Lamar, however, ruled against opening sealed mail, upholding citizens' rights to private correspondence.



1948

> Universal Declaration of Human Rights

The United Nations General Assembly adopted the Universal Declaration of Human Rights. Article 12 emphasized that no individual should endure arbitrary interference in their privacy, family, or correspondence and advocated for legal protection against such violations.

1960

> Privacy Torts Introduced

Legal scholar William Prosser outlined four privacy torts that allow individuals to sue for damages when their privacy is invaded. These include intrusion upon seclusion, public disclosure of private facts, false light publicity, and misappropriation of one's name or likeness.

1967

> Privacy and Freedom by Alan Westin

Alan Westin's seminal book explored the concept of privacy, defining it as the individual's right to control personal information. This work influenced ongoing discussions about technology, privacy, and freedom.



1960s-1970s

1973

> Fair Information Practices (FIPs)

The Records, Computers, and the Rights of Citizens report introduced the principles of Fair Information Practices, which became the foundation for modern privacy laws.

1972

> Keith Case Ruling

The Supreme Court ruled in *United States v. U.S. District Court* that domestic intelligence surveillance required warrants, reinforcing protections against unauthorized government intrusion.

> Landmark Supreme Court Cases

- *Griswold v. Connecticut* (1965): Established marital privacy in matters of contraception.
- *Katz v. United States* (1967): Expanded Fourth Amendment protections to areas where privacy is reasonably expected.
- *Eisenstadt v. Baird* (1972): Extended privacy rights regarding contraception to unmarried individuals.



1974

> FERPA and Privacy Act

The Family Educational Rights and Privacy Act protected students' educational records, while the Privacy Act established rules for federal agencies regarding the handling of personal data.

1986

> TCPA and National Do Not Call Registry

The Telephone Consumer Protection Act and the National Do Not Call Registry were implemented to regulate telemarketing practices and safeguard consumer privacy.



1991

> Common Rule Updates

Ethics standards for human research were updated in the Common Rule, guiding the use of private information in biomedical and behavioral studies.



1998

> COPAA

The Children's Online Privacy Protection Act mandated safeguards for the personal data of children under 13, requiring parental consent for data collection.

1999

> Gramm-Leach-Bliley Act and Chief Privacy Officer

The Gramm-Leach-Bliley Act required financial institutions to disclose data-sharing practices and protect consumer information. Around the same time, corporations began appointing Chief Privacy Officers to manage privacy compliance.

1995

> EU Data Protection Directive

The European Union adopted the Data Protection Directive, establishing comprehensive rules for the processing of personal data. This directive was later replaced by the GDPR.



1996

> HIPAA

The Health Insurance Portability and Accountability Act ensured the confidentiality and security of health-related information while streamlining healthcare data management.

2001

> USA PATRIOT Act

Passed after 9/11, this act expanded government surveillance powers to enhance national security, raising significant privacy concerns.



**GDPR
DATA
PROTECTION**

2012

> EU Right to be Forgotten

The European Commission proposed a regulation granting individuals the right to request the removal of personal information from search engine results.



2003

> Data Breach Notification Laws

California became the first state to require businesses to notify residents of data breaches, inspiring similar laws across the U.S.



2018

> GDPR

The General Data Protection Regulation went into effect in the EU, introducing stringent data protection measures and enhancing individual rights.



2020

> CCPA

The California Consumer Privacy Act provided residents with rights over their personal data, such as access, deletion, and opting out of sales.

2023

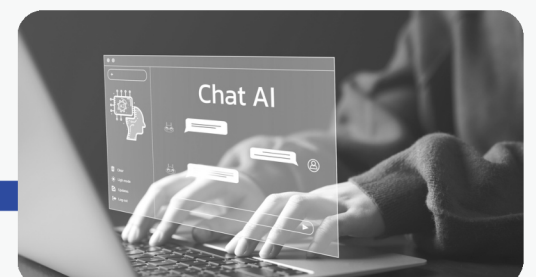
> AI and Privacy Risks

Generative AI became widespread, raising new privacy challenges. The European AI Act was proposed as a framework for AI regulation, categorizing risks into unacceptable, high-risk, and less-regulated applications.

2024

> The EU AI Act

The EU AI Act, the first major regulation of its kind, was introduced to govern AI applications, focusing on risk-based categorizations and protecting fundamental rights.



How can a Data Processor make a Data Fiduciary's life easier under the new DPDP draft rules?



By Mayank Sharma,
Privacy Officer, CRISIL

The Digital Personal Data Protection Act (DPDPA) in India underscores the need for collaboration between Data Fiduciaries and Data Processors to warrant robust compliance. While Data Fiduciaries hold the primary obligation for ensuring safety of collected data and usage, Processors can play a significant role in simplifying the Data Fiduciary's obligations by adopting compliance-focused practices and maintaining transparency in their operations. A crucial starting point is the adoption of a compliance-first approach. Data Processors must design their systems and processes in alignment with DPDPA's core principles, such as purpose limitation, transparency, data minimization, and lawful processing. This proactive alignment reduces the oversight burden on Data Fiduciaries. Moreover, a well-drafted Data Processing Agreement (DPA) is critical for defining roles and responsibilities. This agreement should address key aspects like processing purposes, security measures, breach notification protocols, and sub-processing restrictions, providing Data Fiduciaries with clarity and control over data management.

Ensuring robust data security measures is another area where Data Processors can add immense value. By adopting best practices like encryption, data masking, privacy by design, pseudonymization, and regular penetration testing, Data Processors not only safeguard personal data but also provide Data Fiduciaries with assurance against potential regulatory risks. Compliance with internationally recognized standards, such as ISO 27001, 27701 (PIMS) or SOC 2, further strengthens this assurance. Regular audits by the Data Processors help Data Fiduciaries monitor compliance without excessive intervention.

Data Processors can also assist Data Fiduciaries in addressing Data Principal requests effectively. Mechanisms to quickly retrieve or delete personal data ensure Data Fiduciaries meet statutory obligations with ease. Additionally, robust incident management protocols, including timely breach reporting and remediation measures, allow processors to support fiduciaries in maintaining regulatory compliance during critical situations.

By fostering a partnership built on trust, transparency, and adherence to regulatory mandates, Data Processors can significantly ease the Data Fiduciary's compliance burden. This collaboration not only ensures better adherence to the DPDPA but also lays the foundation for a robust data protection ecosystem where accountability and trust thrive. As India's data protection landscape evolves, such partnerships will become even more indispensable.

Disclaimer: The opinion expressed here is solely my own and not associated with my employer.

Third party risk management under the 2025 draft rules



By Kartikeya Raman
Associate Partner, Digital Trust and Transformation, Forvis Mazars, India

The DPDP Draft Rules in India highlight the critical importance of effective third-party risk management for Data Fiduciaries. Rule 6(b) emphasizes that Data Fiduciaries must implement strong access control measures for both their own computer resources and those used by third-party Data Processors. This ensures that only authorized personnel have access to sensitive personal data, reducing the risk of unauthorized access or data breaches when third parties are involved in processing. In addition, Rule 6(f) mandates that Data Fiduciaries include provisions in their contracts with Data Processors for reasonable security safeguards. These provisions should outline data protection protocols, breach response measures, and other safeguards to ensure that third-party processors maintain a level of security comparable to that of the Data Fiduciary. Such contractual agreements are critical to ensuring that third-party Data Processors are legally bound to uphold data protection standards and respond effectively in the event of a breach. Together, these rules emphasize the need for both technical and contractual measures to mitigate the risks associated with third-party data processing.

contractual measures to mitigate the risks associated with third-party data processing.

By ensuring that Data Fiduciaries adopt strong access controls and establish secure contracts with Data Processors, the DPDP framework aims to safeguard personal data from potential misuse or unauthorized access. Non-compliance with these requirements could result in significant regulatory consequences for Data Fiduciaries, including penalties or suspension of registration, as set out in other provisions of the DPDP framework. This underscores the need for Data Fiduciaries to manage third-party relationships with due diligence and accountability.

How Should Companies (Data Fiduciaries) Approach Parental Consent?



By Sindhu Vethoddy
Managing Director, Protiviti

Data privacy goes beyond being a mere legal obligation as it serves as a critical foundation for safeguarding individual autonomy and maintaining public trust in the digital age. Children, by virtue of their age and developmental stage, have limited awareness, which necessitates additional protections to prevent the exploitation, misuse or unauthorized sharing of their personal information. Parental consent plays a critical role here, especially in situations where Data Fiduciaries collect or process personal information from minors. Handling children's data responsibly not only fulfills legal obligations but also safeguards the rights and well-being of these vulnerable individuals, reinforcing ethical and responsible practices in the digital ecosystem.

First and foremost, businesses and governments must recognize and understand the rationale behind the stringent requirements of global children's privacy laws, such as the U.S. Children's Online Privacy Protection Act (COPPA) and the EU's General Data Protection

Regulation (GDPR), in safeguarding minors' data. Considering the foundational principles of such regulations that prioritize children's safety, the Government should reevaluate the sweeping compliance exemptions granted for processing children's data under the DPDP Rules, 2025. Designing a clear consent process and verifying guardians requires a balance between simplicity, transparency and security. Transparent notices should explain data collection practices in simple terms, accessible to both children and their guardians. Parental consent verification can be achieved through methods such as government-issued ID submission, email verification or a court-issued document. Additional measures, like real-time video interactions, digital signatures or trusted third-party authentication, can further enhance reliability. To enhance the standard practice, Data Fiduciaries could implement dynamic consent mechanisms that allow parents to monitor, modify or revoke their consent as needed.

Additionally, leveraging advanced privacy-enhancing technologies such as pseudonymization or encryption at the collection stage can further safeguard the data. Establishing clear access logs and audit trails, which parents can review upon request, adding an extra layer of transparency ensuring stronger security. Finally, companies should remember that parental consent is not static. Situations change and children grow older. Managing evolving parental consent can be achieved through consent dashboards for updates, multi-factor authentication for secure verification, AI-powered age checks, encrypted tokens for tracking, collaboration with trusted institutions and periodic revalidation via automated reminders. In conclusion, parental consent is a vital element of data privacy, especially when dealing with minors' data. By combining clear processes, robust verification methods and adaptive consent mechanisms, businesses can ensure compliance, protect children's rights and foster trust in the digital ecosystem.

What's missing in the DPDP draft rules?

The Digital Personal Data Protection (DPDP) Rules, while significant, contain several critical gaps that could impede effective implementation. The most pressing concerns revolve around three main areas:

THE CONSENT MANAGER FRAMEWORK FACES PRACTICAL CHALLENGES.

While it's designed to help users manage their consent across multiple data fiduciaries, there's no clear standard for personal data taxonomy, no mechanism to track which entities hold user data. There is no clear path for extending the consent manager framework beyond financial data to areas such as health records.

THE CLASSIFICATION OF

SIGNIFICANT DATA FIDUCIARIES (SDFS) LACKS CLARITY.

The Rules don't define what constitutes "high volume" or "sensitive" data, leaving organizations uncertain about whether they qualify as SDFs or not. This ambiguity affects compliance planning and implementation.

THE PROCESSING OF CHILDREN'S DATA PRESENTS SIGNIFICANT OPERATIONAL CHALLENGES.

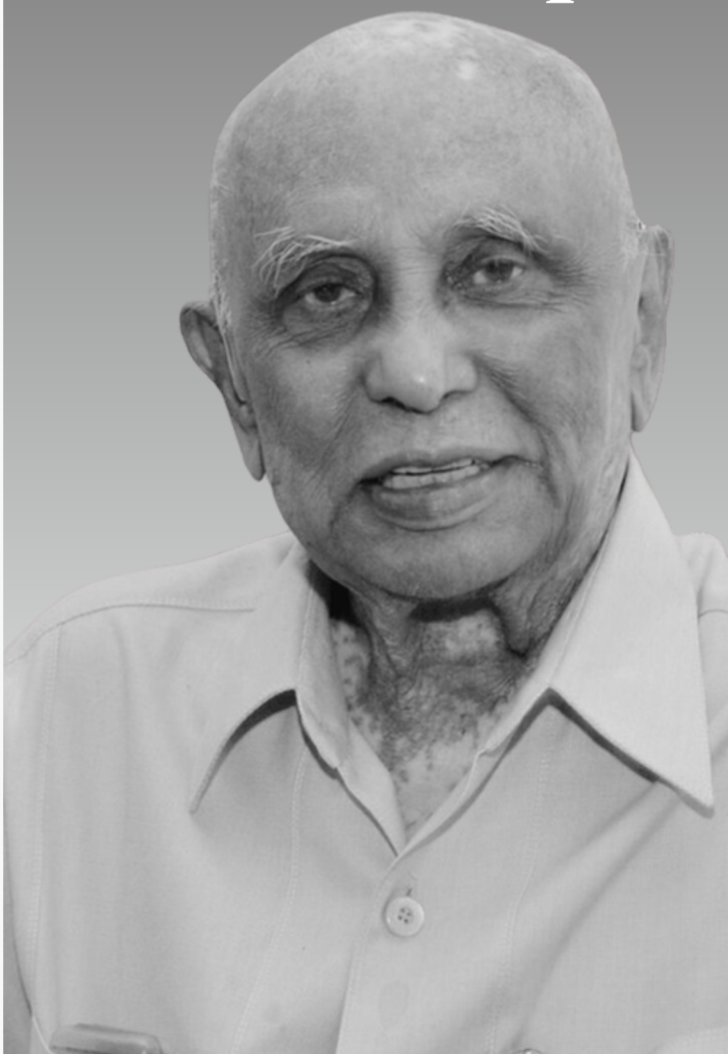
The Rules require age verification and parental consent but don't provide practical mechanisms for implementation. There's no clear way to verify a

minor's age or authenticate parental relationships, especially when parents aren't users of the platform.

Additional gaps include unclear timeframes for processing requests, undefined workflows for data erasure and portability, lack of specific formats for breach notifications, and ambiguous consent formats. The Rules also defer cross-border transfer specifics to future government orders, creating uncertainty for global businesses. These ambiguities and operational gaps could create significant hurdles for businesses and privacy advocates, necessitating further refinement through stakeholder engagement.



TRIBUTE TO JUSTICE K.S. PUTTASWAMY *And His Impact on the Privacy Landscape*



By Debashree Mukherjee
Director, PW&CO. LLP

The Supreme Court's historic ruling in Justice K.S. Puttaswamy (Retd.) vs Union of India has had a far-reaching impact on privacy in India. By affirming the right to privacy as a fundamental right under Article 21 of the Constitution, the judgment laid a solid foundation for the protection of personal data in the digital age. Justice K.S. Puttaswamy's principles on privacy emphasized the right to privacy as fundamental, consent-based data processing, data minimization, and transparency in data handling. His recommendations also called for strong safeguards against surveillance, rights to access and erase personal data, and the establishment of an independent Data Protection Authority. These principles significantly influenced India's 2020-2022 privacy bills and contributed to the 2023 Digital Personal Data Protection Act.

In light of this judgment, the Government of India took concrete steps to establish a privacy-focused legal framework. The impact of the ruling is evident—around six years later, India enacted the Digital Personal Data Protection Act, 2023 (DPDPA), a new data protection legislation aimed at strengthening privacy protections in the country.

The key principles of the DPDPA are consent and giving individuals control over their personal data. It requires organizations to obtain consent, explain how data will be used in simple terms, and protect the rights of individuals. The DPDPA emphasizes that data processing must be legal and provides clear ways for individuals to manage their personal information. In particular, the DPDPA requires organizations to provide clear and easy-to-understand information about how personal data is collected, used,

and retained, allowing individuals to make informed decisions regarding their data.

The enactment of the DPDPA marks a significant shift in India's approach to data privacy, aligning with the Supreme Court's emphasis on safeguarding personal data. By introducing stringent data security provisions, the DPDPA ensures that organizations must implement robust technical and organizational measures to protect personal data from misuse, breaches, and unauthorized access. These provisions not only address the Court's concerns about data misuse but also highlight the growing importance of transparency and accountability in data processing. With these changes, individuals will have greater control over their personal information, and organizations will be held accountable for upholding privacy standards, ultimately fostering a more secure and trustworthy digital ecosystem.

Consent Managers: Critical, But Not Mandatory Under the DPDP Act

ASHOK HARIHARAN, CEO - IDfy

What are your views on consent managers as per the recently released draft rules?

"Consent managers, as outlined in the DPDPA, are undoubtedly a significant innovation for managing data privacy. They empower data principals to manage, review, and withdraw consent across fiduciaries in a consolidated manner. This capability is vital for fostering trust and transparency in digital ecosystems. However, it's critical to note that consent managers must be Indian entities, ensuring they operate under domestic jurisdiction and regulatory oversight."

Are consent managers mandatory for fiduciaries to obtain consent from their customers?

"The answer is straightforward: consent managers are not mandatory for either fiduciaries or data principals under the DPDP Act. The Act clearly allows data principals the choice to give, manage, or withdraw consent through a consent manager. The emphasis here is on

flexibility, making consent managers an optional tool rather than a regulatory requirement.

Fiduciaries, however, are obligated to ensure that consent processes are transparent and well-documented. As per the Act, if the validity of consent is questioned, fiduciaries must demonstrate that a proper notice was issued and explicit consent was obtained. This means fiduciaries can directly seek consent from data principals, provided they follow the guidelines established under frameworks like DEPA and MeitY's electronic consent protocols. By maintaining clear, auditable trails of all consent activities, fiduciaries can fulfill their legal obligations without depending on consent managers."

If consent managers are subservient to the data principal, how can individuals fully exercise their rights in the absence of consent managers?

"Even without a consent manager, data principals can fully exercise their rights through the

Data Principal Rights Management (DPRM) portal provided by fiduciaries. This includes rights such as viewing and revoking consents, addressing grievances, and submitting access or correction requests. Fiduciaries are responsible for ensuring these rights are accessible, seamless, and user-friendly. By maintaining electronic records of consent and leveraging the DPRM, fiduciaries can create a robust mechanism for data principals to exercise their rights efficiently, even without a consent manager."

What is the biggest challenge that you foresee for consent managers?

"The absence of open standards for consent managers is a critical challenge. Ideally, consent managers would allow data principals to view and manage all consents given across fiduciaries in one unified place. However, such interoperability remains elusive.

For example, the Account Aggregator (AA) framework launched in 2016 is yet to achieve

universal adoption among banks due to the lack of open standards. Similarly, without open standards for consent managers, data principals may find themselves navigating individual DPRM portals of various fiduciaries to manage

their consents—a fragmented and cumbersome process. This underscores the importance for fiduciaries to prioritize consent governance internally, ensuring a seamless user experience while the ecosystem around consent managers matures."



Navigating Trust & Privacy: A MASTERCLASS ON DPDPA COMPLIANCE (2025)

Here's what you will learn:

- ✓ Managing Data Principal rights
- ✓ Guide for Data Processor Management
- ✓ Basics of the DPDP Act 2025
- ✓ How to implement the DPDP Act 2025
- ✓ Duties of a Data Protection Officer

Bonus: The course features exclusive insights from **Supratim Chakarborty, Partner at Khaitan and Co. and Vinayak Godse, CEO at DSCI.**

3 Hour Certified course!

Limited Time Offer: Get 90% OFF
using the code **PRIVY90** at checkout!
Start learning by scanning this code!



Instructor

Nikhil Jhanji

DSCI-certified DPO, IDfy



Supratim Chakraborty
Partner, Khaitan & Co.



Vinayak Godse
CEO, DSCI



Ashok Hariharan
CEO, IDfy

Who is this course for?

For **CISOs** who've seen it all, **DPOs** who mean business, and **privacy professionals** who appreciate a solid game plan.

Horoscope

CISO



The stars have aligned to put you in the spotlight! Your security expertise is now more crucial than ever under DPDP. The cosmos brings heightened responsibilities around data protection, but also unprecedented support from management. Those security frameworks you've been championing? They're finally getting the attention they deserve. Expect sleepless nights as you fortify defenses, but your efforts will establish you as the guardian of digital trust. Watch for opportunities to collaborate with the DPO – this cosmic partnership will be key to your success!

DPO



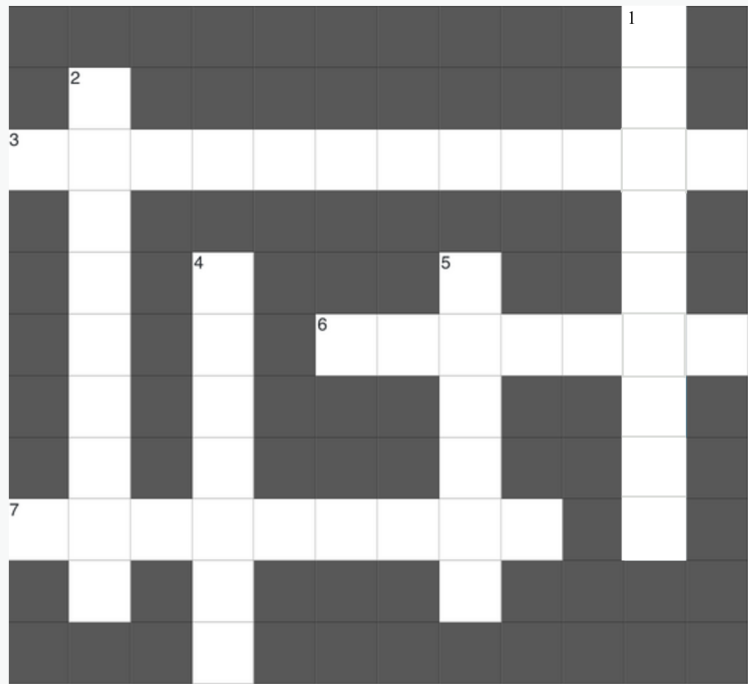
The universe has chosen you as its newest protagonist! Your role emerges as a critical cornerstone of organizational compliance. The stars predict countless meetings as you become everyone's favorite consultant. Your inbox will overflow with privacy queries, but fear not – your expertise in navigating DPDP's complexities will earn you respect across departments.

CTO



The tech cosmos is undergoing a major shift, dear CTO! The DPDP brings both challenges and opportunities to your digital realm. Mars' position suggests intensive architecture reviews as privacy-by-design becomes your new north star. Your tech stack will need evolution – the stars predict heated discussions about data localization and storage limits. Your biggest challenge? Balancing legacy systems with new privacy requirements.

Crossword



Across:

- 3 Rule 4(b) requires data fiduciaries to collect data that is strictly necessary for the specified purpose. (12)
- 6 Rule 5 requires this to be clearly stated before collecting or processing any personal data. (7)
- 7 Rule 9 mandates that fiduciaries must establish mechanisms to address this from data principals. (9)

Down:

- 1 Rule 2(1)(m) designates this entity to process personal data on behalf of a fiduciary. (9)
- 2 As per Rule 2(1)(i), this entity determines the purpose and means of processing personal data. (9)
- 4 Defined in Rule 3 of the DPDP 2025, this must be free, informed, specific, and unambiguous for any processing of personal data. (7)
- 5 As per Rule 7 of the DPDP 2025, this must be reported to the Data Protection Board and affected individuals in case of unauthorized access or misuse of personal data. (6)

Solutions

- CROSSWORD
- Across:
- 3. Minimization 6. Purpose
 - 7. Grievance
- Down:
- 1. Processor 2. Fiduciary
 - 4. Consent 5. Breach

SUDOKU

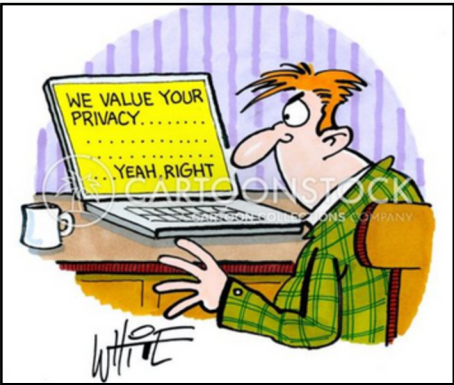
3	1	7	2	4	9	6	5	8
2	6	5	7	8	3	4	9	1
9	4	8	1	6	5	7	2	3
8	5	4	6	9	2	1	3	7
7	2	3	4	1	8	9	6	5
1	9	6	5	3	7	8	4	2
4	7	2	9	5	1	3	8	6
6	8	1	3	2	4	5	7	9
5	3	9	8	7	6	2	1	4

To solve the sudoku, each row, column and box must contain the numbers 1 to 9

Sudoku

		3				6			4
6			1			2	4		7
4						1		3	
			6	5	3			8	4
7			3		1			6	5
		5		6	9			3	7
9			8	1				7	
				7					
			7		4				5

Just For Laughs



No picking and choosing!

Ut not ad minim veniam, quis nostrud
callamco for nisi ut aliquip ex ea
conmodo consequat. Duis aute dolor in
reprehenderit in voluptate sale

dolore seu fugiat nulla pariatur. Excepteur sint
dolore et dolore magna aliqua enim culpa
qui officia deserunt mollit anim id est laborum.

**Your Consent Notice
must cover specified purposes.**

Priview

