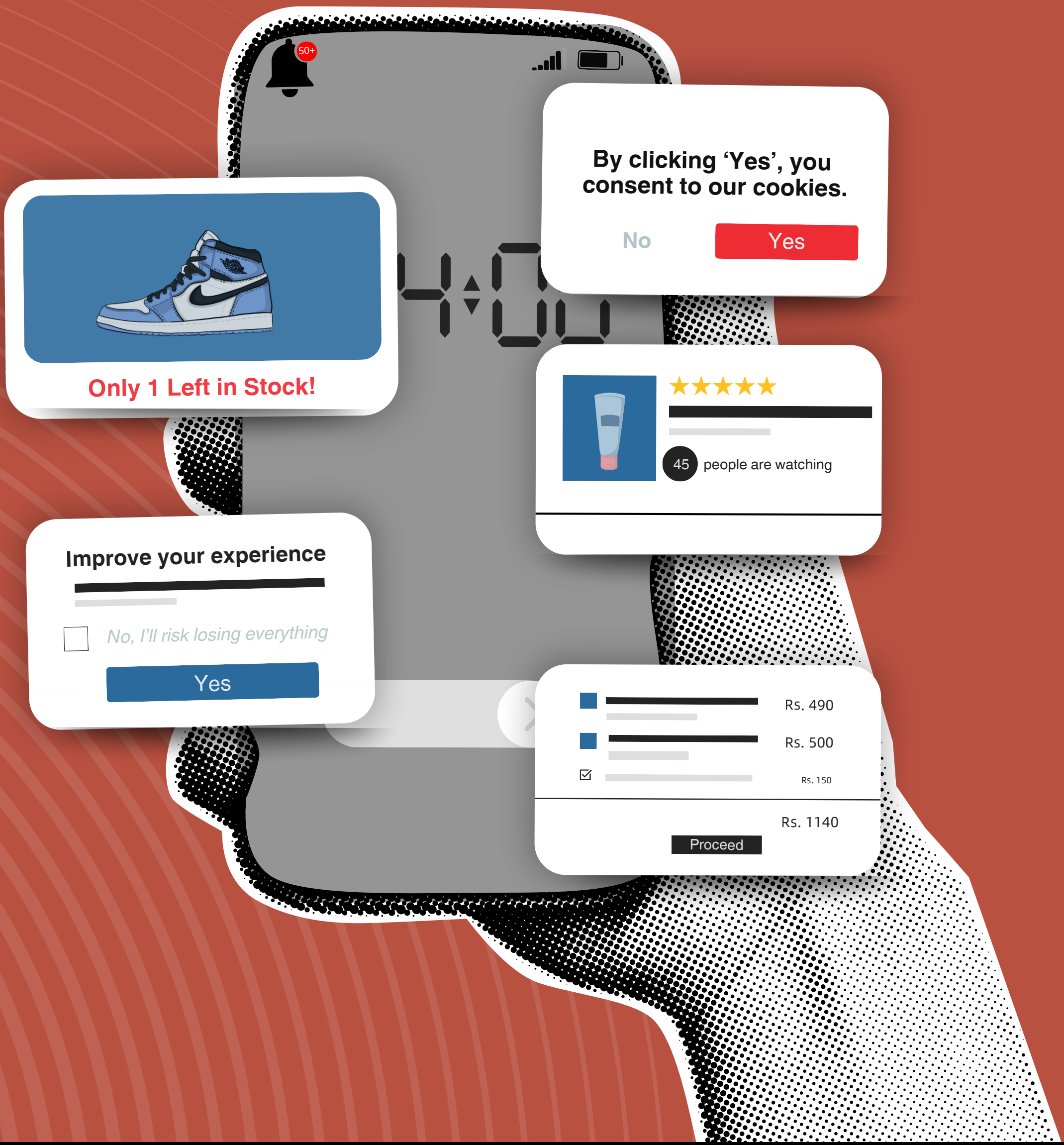
Policy Brief

Manipulative Consent: Analysing Draft Digital Personal Data Protection Rules, 2025



2025 MARCH

CENTER FOR LAW AND CRITICAL EMERGING TECHNOLOGIES,
ADVANCED STUDY INSTITUTE OF ASIA

ADVANCED STUDY INSTITUTE OF ASIA

The Advanced Study Institute of Asia (ASIA), founded in 2023 and affiliated with Shree Guru Gobind Singh Tricentenary University in Gurugram, is a think tank dedicated to making sense of the shifting political, economic, and social landscape of South and Southeast Asia.

CENTER FOR LAW AND CRITICAL EMERGING TECHNOLOGIES

Center for Law and Critical Emerging Technologies (CLET) is a research initiative under ASIA that examines the vulnerabilities and challenges of rapidly evolving, interconnected technologies, exploring their economic, political, and ethical implications. Its work spans critical areas such as intellectual property, digital governance, and emerging tech policy. Recent initiatives include the Progress and Policy Roundtable on Standard Essential Patents (SEPs) and research projects like the Quantum Index and Dark Pattern Report. At its core, CLET aims to foster global collaboration and drive research on innovation in an increasingly complex technological landscape.

INTERNET FREEDOM FOUNDATION

Internet Freedom Foundation ("IFF") is a registered charitable trust that works to advance constitutional guarantees in India, especially as they relate to digital rights and freedoms, through strategic litigation, government engagement, and civic advocacy.

Authors:
Shivani Singh (Programme Coordinator, CLET, ASIA)
Farheen (Policy & Research Analyst, ASIA)

Advisors: Prof. Amogh Rai, Abhilasha Semwal, Medha Garg & Apar Gupta (Internet Freedom Foundation), Karthika Rajmohan.

For further inquiries, collaborations, or permissions, please contact:
📧 communication@advancedstudy.asia
🌐 https://asiaresearch.co/

Disclaimer: The views expressed in this research note are personal views of the author(s) and do not necessarily reflect the views of Internet Freedom Foundation

POLICY BRIEF

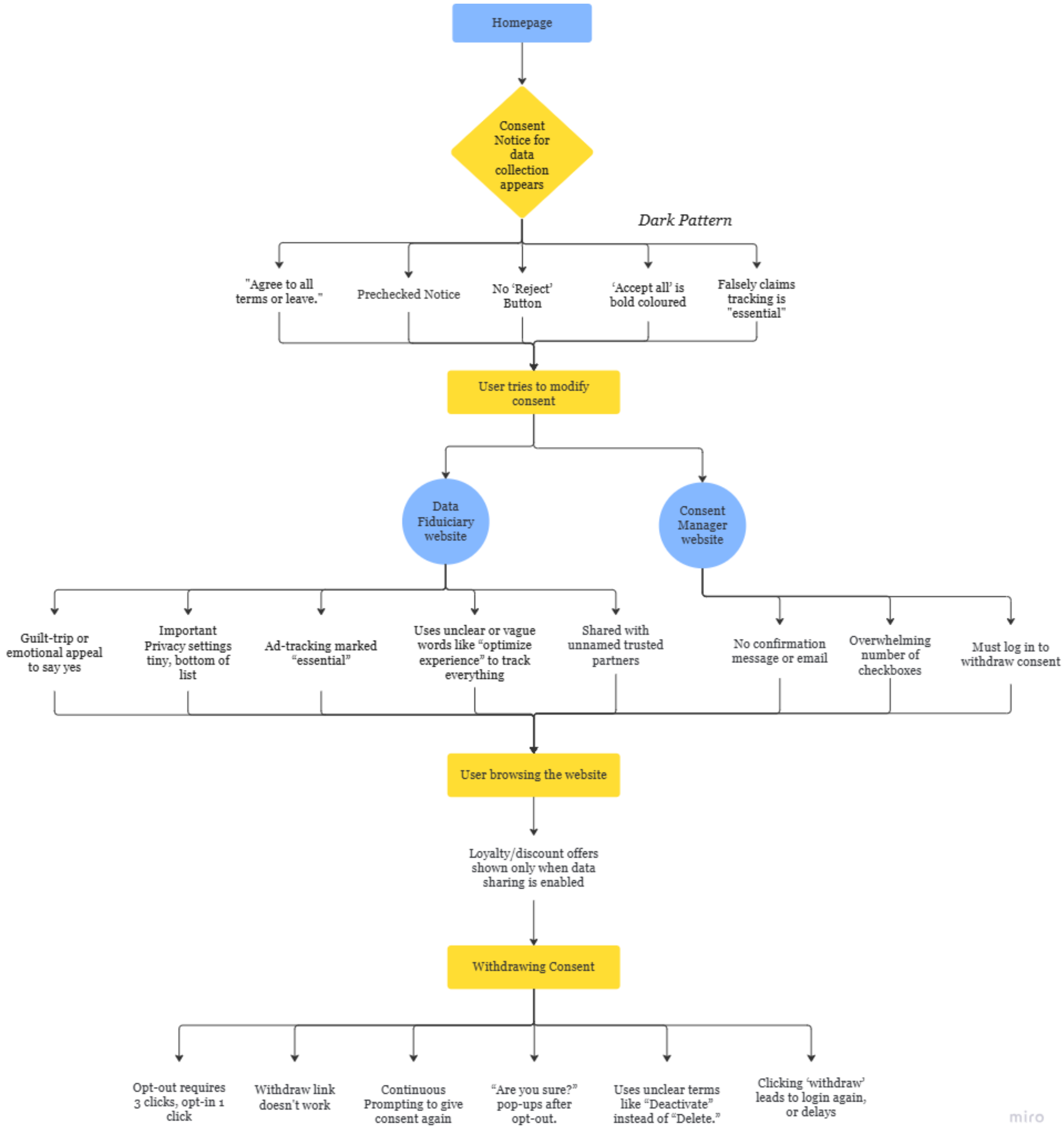
ANALYSING DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

This policy note responds to the Draft Digital Personal Data Protection (DPDP) Rules, 2025. While the framework aims to empower users, key enforcement and gaps remain.

Key Points:

1. **Consent is not genuinely free or informed:** Although the DPDP Act, 2023 and the draft rules mandate that consent be "free, informed, specific, and unambiguous," in reality, digital platforms employ manipulative user interface (UI) designs and dark patterns (such as pre-checked boxes, confusing language, or concealed opt-outs) that push users into consenting without fully realizing their decision. Such UI practices are not prohibited yet under the law.
2. **Several regulatory loopholes still persist:** The legislation leaves out critical holes such as the revenue model and non-partisanship of consent managers, unregulated for renewed parental consent, non-transparency over secondary processing of data (e.g., AI profiling), and no certain protection from algorithmic discrimination or misuse. These gaps erode user privacy and confidence.
3. **Need for convergence of regulations:** India's dispersed legal framework makes it easier for companies to take advantage of gaps in regulation between data protection legislation and consumer protection regulations. The DPDP regime needs to converge enforcement activities with bodies such as consumer protection authorities, prospective Artificial Intelligence (AI) regulators, and industry regulators.

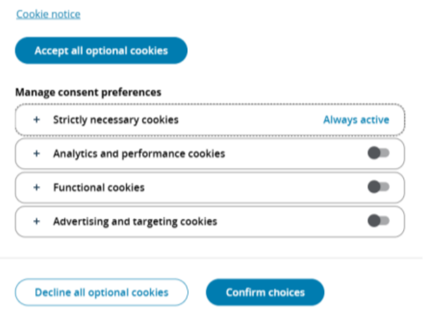
Figure 1. How Dark Patterns Slip Through DPDP:


Homepage
Consent Notice for data collection appears
Dark Pattern
"Agree to all terms or leave."
Prechecked Notice
No 'Reject' Button
'Accept all' is bold coloured
Falsely claims tracking is "essential"
User tries to modify consent
Data Fiduciary website
Consent Manager website
Guilt-trip or emotional appeal to say yes
Important Privacy settings tiny, bottom of list
Ad-tracking marked "essential"
Uses unclear or vague words like "optimize experience" to track everything
Shared with unnamed trusted partners
No confirmation message or email
Overwhelming number of checkboxes
Must log in to withdraw consent
User browsing the website
Loyalty/discount offers shown only when data sharing is enabled
Withdrawing Consent
Opt-out requires 3 clicks, opt-in 1 click
Withdraw link doesn't work
Continuous Prompting to give consent again
"Are you sure?" pop-ups after opt-out.
Uses unclear terms like "Deactivate" instead of "Delete."
Clicking 'withdraw' leads to login again, or delays
miro

1. Consent is Not Yet Free:

The Digital Personal Data Protection (DPDP) Act, 2023, along with the 2025 rules, establishes a framework for data protection in India. The law states that consent must be "free, specific, informed, unconditional, and unambiguous," and that withdrawing consent should be just as easy as giving it. On paper, this seems strong. But in practice, it leaves gaps that allow data fiduciaries (companies) to exploit it.

The law requires that notices for consent be clear, but in reality, they rarely are. Any choice made on digital platforms is influenced by how it is presented, designed, and the effort required to take action. Over the years, digital platforms have refined their interfaces to guide users toward actions that benefit them. This is heavily researched in literature as dark pattern or sludges, designed to add friction to specific action or nudge user towards specific choice that benefits the data fiduciary. Some examples of these are listed below.



Cookie notice

Accept all optional cookies

Manage consent preferences

+ Strictly necessary cookies Always active

+ Analytics and performance cookies ○

+ Functional cookies ○

+ Advertising and targeting cookies ○

Decline all optional cookies Confirm choices

Dark patterns, design tricks that push users toward decisions they might not otherwise make, are key to this problem. Although the Digital Personal Data Protection (DPDP) Act, 2023 calls for consent to be "free, informed, specific, and unambiguous" (Section 6), it does not specifically forbid manipulative interface design. Rule 3 requires notice in "clear and plain language," but it ignores coercive UI techniques including bold "Accept," hidden "Reject," links, or confirmshaming.

This results in a paradox: platforms can theoretically comply while yet erasing privacy via interface fatigue, confusing decisions, or manipulative flows. The Act notes "ease of withdrawal" (Rule 3(c)) but does not guarantee equal visibility or friction for rejecting permission. Most importantly, overcollecting is justified by stating the goal; there is no need to restrict the volume of data acquired. Consent Managers run the danger of being tools of subtle coercion without guidelines on design fairness or behavioural nudging. The law promises control, but its silence about dark patterns leaves actual user autonomy unprotected. Consent to mean anything requires design to be included in the rules.

Consider e-commerce platforms that pre-select extra charges at checkout, assuming users won't notice. Or loan apps that make opting out feel like a mistake with phrases like "No thanks, I don't want to improve my financial future." Travel sites use fake urgency, "Only 2 left in stock!", to pressure users into acting fast. These techniques are not about transparency. They are about steering users toward choices that benefit businesses, not individuals.

This is not just a technical flaw. It is a question of whether privacy is treated as a fundamental right or a negotiable preference. The Justice K.S. Puttaswamy case (2017) established privacy as a core constitutional right, yet the DPDP Act does not guarantee privacy by default. Unlike the EU's GDPR, which ensures users must opt in before data collection begins, India's law allows platforms to collect data unless users actively opt out. The burden is placed on individuals to protect their own privacy, rather than on companies to respect it.

If the law is to be truly effective, it must go further. Consent should not just be easy to withdraw, it should be difficult to obtain unfairly. Companies should not be allowed to use pre-checked boxes, misleading design, or unnecessary complexity to make opting in easier than opting out. Privacy settings should be simple, accessible, and default to protection, not exposure. Cookie banners should provide a single-click rejection option, just as they provide a single-click acceptance. And penalties should apply not just for failing to obtain consent, but for obtaining it in ways that obscure, confuse, or pressure users.

2. Loopholes Yet to Be Covered

While the DPDP Rules lay out the process for consent and data handling, several quiet loopholes remain. Consent Managers are positioned as neutral intermediaries but are actually private companies with no defined revenue model. This creates uncertainty about whether their choices serve the user or the platform. There's also no rule for renewing parental consent as children grow older or for handing over data control once they become adults. Further, the Rules don't clarify how personal data is used in automated decision-making or algorithmic profiling. Without transparency, users may be affected by AI systems without knowing how or why. These may seem like technical gaps, but they shape everyday user experience and trust in the system. To ensure meaningful privacy, these small but important details must be addressed.

For a full list of rule-specific gaps and proposed amendments, please refer to the Annexure.

3. Need Convergence of regulations:

India's legal framework for data protection is fragmented. DPDP Act duplicates other legislation such as the Consumer Protection Act (CPA), Bureau of Indian Standards (BIS) norms, and draft guidelines laid down for Artificial Intelligence (AI). But since these rules do not work in tandem with each other, companies seek loopholes to evade actual accountability.

For instance, the CPA safeguards consumers from deceptive business conduct but not necessarily privacy. In contrast, the DPDP Act is privacy-conscious but weak in consumer rights safeguards. This gives companies an ability to profess obedience to one system of rules but disregard another. A retailer may assert its data gathering practices align with DPDP legislation while pursuing aggressive marketing campaigns that are legally within consumer protection legislation. Similarly, e-commerce companies that claim to self-regulate often set rules that favor their own interests rather than truly protecting users.

To fix this, India needs a coordinated approach where data protection and consumer rights enforcement go hand in hand. This means connecting the DPDP Authority, consumer protection agencies, and industry regulators to close loopholes. Compliance measures should also be made standardised so companies can't switch between various legal paradigms to avoid culpability. Moreover, harsher penalties should be introduced for those companies that engage in manipulation of consent or wrongfully use personal data. The EU's GDPR already does this, charging companies up to 4% of global revenue as a fine for violations. India must take such measures so that companies will treat data protection seriously.

The other major enforcement challenge is ensuring compliance with the rules by companies of all sizes. Large enterprises tend to have the funds to afford compliance, but SMEs might not be able to cope. The question therefore arises whether regulatory agencies should offer assistance mechanisms in the form of guidelines, templates, and compliance training programs to enable SMEs to conform to data protection legislation without undue economic cost. The intention should be to build a compliance culture and not only punish those who do not comply with the rules.

The DPDP Act is a necessary step in India's digital regulation, but it cannot afford to be passive, procedural, or naïve about the ways companies extract consent. A policy is only as strong as its enforcement, and right now, the rules don't protect users from the reality of how digital consent is manufactured.

If data is power, then users should not have to fight to reclaim it.

ANNEXURE-1

OFFICIAL RECOMMENDATIONS FOR DRAFT DIGITAL PERSONAL DATA PROTECTION (DPDP) RULES, 2025

Sl. No.	Rule	Comments/Suggested Changes
1	**Rule 2** (Definitions)	**Lack of definition for dark patterns:** Rule 2 does not explicitly define "dark patterns," which may lead to ambiguity in interpretation and enforcement. It would be beneficial for the draft Digital Personal Data Protection Rules, 2025 ("draft Rules") to incorporate a clear definition. This would help ensure in recognising and regulating manipulative online practices.
2	**Rule 3** (Notice given by Data Fiduciary to Data Principal)	**Lack of safeguards against dark patterns in consent mechanisms:** Rule 3 does not explicitly address the risk of dark patterns influencing how consent is obtained, which may lead to manipulative practices by data fiduciaries. Currently, the draft Digital Personal Data Protection Rules, 2025 (“draft Rules”) do not specify the mode of obtaining consent, leaving it entirely to the discretion of the data fiduciary. This creates room for deceptive interfaces that nudge users into providing more personal data than necessary. To ensure that consent is truly free and informed, the Rules should require clear and granular consent mechanisms, allowing users to selectively opt in or out of different types of data processing. Take-it-or-leave-it consent models, forced actions, and cognitive overload in consent interfaces should be explicitly prohibited. For instance, an e-commerce platform should not bundle consent for marketing promotions and data sharing with third-party advertisers into a single acceptance. Additionally, the Rules should align with existing consumer protection frameworks, such as the Consumer Protection Act, 2019 (CCPA) – Information Clarity Mandates, and incorporate relevant industry guidelines. The Bureau of Indian Standards (‘BIS’) has issued a draft standard titled E-commerce – Principles and Guidelines for Self-Governance, which provides self-regulatory guidelines addressing dark patterns. Aligning the Rules with such best practices would strengthen consumer protection and prevent manipulative consent practices.
3	**Rule 3**(Notice given by Data Fiduciary to Data Principal)	**Lack of transparency in secondary data use:** Rule 3 requires Data Fiduciaries to provide notice to Data Principals regarding the purpose of data collection. However, the rule does not mandate disclosure of secondary uses of data, such as profiling, AI model training, selling of data, or cross-device tracking. This creates a significant gap in transparency, as users may consent to data collection for one purpose without realising that the same data is later used for unrelated activities. For instance, a social media platform may inform users that their data is being collected to “improve services” without explicitly

		disclosing that it is also used for political profiling, targeted advertising, or resale to data brokers. To prevent such deceptive practices, the Rules should require Data Fiduciaries to provide complete disclosure of all secondary purposes and offer users the ability to opt out of each distinct processing activity. Furthermore, data collected should not be used for purposes that amount to unfair trade practices or restrictive trade practices under the Consumer Protection Act, 2019. Users must have clarity on how their data will be utilised beyond its immediate purpose, ensuring that their consent is meaningful and aligned with the principles of fair data processing.
4	**Rule 3**(Notice given by Data Fiduciary to Data Principal)	Rule 3 mandates informed consent but does not specify how consent interface design affects user choices. Conventional tick-box models often lead to "click fatigue", where users blindly accept terms. Without clear design guidelines, platforms may use complex notices, bundled consents, or manipulative layouts that discourage genuine decision-making. To ensure meaningful engagement, the Rules should encourage interactive consent models such as drag-and-drop selections, swiping gestures, or step-based disclosures to prevent cognitive overload. Users should also have real-time options to modify or revoke consent, rather than a static one-time approval.
5	**Rule 3**(Notice given by Data Fiduciary to Data Principal)	**Excessive information burden in consent notices:** Rule 3 requires Data Fiduciaries to provide notices to Data Principals regarding data collection and processing. However, the current framework places excessive responsibility on users to navigate complex and overwhelming information disclosures. This can lead to decision fatigue, where individuals either provide blanket consent without fully understanding its implications or disengage entirely. To address this, the Rules should mandate a privacy by design approach that minimises unnecessary and repetitive consent requests. Notices should be structured to ensure that users receive clear, relevant, and easily digestible information. This aligns with the DPDP Act, 2023 – Section 5 (Notice Requirements) and the Consumer Protection Act, 2019 (CCPA) Guidelines on Information Clarity. Additionally, consent notices should link each category of collected personal data to a clearly stated purpose. For example, if an app collects location data, the notice should explicitly state whether it is for navigation assistance, targeted advertising, or analytics. This will help Data Principals quickly understand how their data is being used and enable them to make informed choices without being overwhelmed by unnecessary details.
6	**Rule 4** Obligations of Consent Manager	A Consent Manager shall not employ or facilitate the use of dark patterns that coerce, mislead, or manipulate Data Principals into consenting to data processing. This includes, but is not limited to, pre-selected consent options, misleading UI elements, unnecessarily complex withdrawal mechanisms, and any deceptive practices as defined in the Guidelines for Prevention of Dark Patterns, 2023.
7	**Rule 4** Obligations of Consent Manager	Rule 4 defines the obligations of Consent Managers but does not mandate a uniform and interoperable consent management process. This lack of standardisation forces users to navigate multiple, non-uniform consent revocation processes across different platforms, leading to consent fatigue

		and inefficiencies. To address this, Rule 4 should require: (i) A standardised consent revocation process across platforms, ensuring that users can manage their data permissions in a consistent and predictable manner; (ii) Interoperability through API-based consent management, where users can modify their consent preferences across multiple services through a unified dashboard; (iii) A single-toggle revocation mechanism, preventing Data Fiduciaries from creating friction-based deterrents to withdrawing consent. These measures align with the Consumer Protection Act, 2019 (Fair Digital Practices) and global best practices such as the European Data Protection Board's consent portability guidelines. Establishing a uniform, user-friendly approach will help reduce consent fatigue, enhance user autonomy, and ensure a seamless consent management experience.
8	**Rule 10** Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian	Rule 10 does not require periodic renewal of parental consent, which may not reflect the evolving preferences of the child as they mature. A 13-year-old may have their data processed with parental consent, but by the age of 17, they may wish to exercise their own rights over their personal data. To address this, the regulation should mandate biennial revalidation of consent and, upon attaining 18 years of age, the Data Principal should be notified and granted full control over their data, including the right to withdraw earlier parental consent. Section 9 of the DPDP Act, 2023, states that data collection cannot be detrimental to the well-being of a child. To reinforce this protection, Rule 10 should also include restrictions on dark patterns, profiling, and targeted advertising for children. While these obligations should apply broadly, they should be stricter for children to prevent exploitation of their digital vulnerabilities. Additionally, although robust parental consent and age verification mechanisms are ideal, their implementation poses risks to children's data privacy, as excessive personal data may be collected. The regulation should aim for a balance between compliance and minimising unnecessary data collection to ensure children's privacy is protected.
9	**Rule 10**	The rule does not place any limit on secondary use of children's data. The regulation must impose purpose-specific consent and ban Data Fiduciaries from performing secondary processing on children's data without express opt-in by the guardian or child when they turn a specific age.
10	**Rule 12** Additional obligations of Significant Data Fiduciary	Regulatory exemptions should not allow large firms to bypass compliance by operating through smaller subsidiaries. Regulatory arbitrage risks should be addressed by extending algorithmic accountability requirements to all firms handling large-scale user data.
11	**Rule 12** Additional obligations of Significant Data Fiduciary	**Lack of transparency in algorithmic decision-making & Need for consumer rights safeguards:** Rule 12(3) does not impose clear transparency obligations on Significant Data Fiduciaries (SDFs) that use AI or algorithmic systems to process user data. Currently, there is no requirement for SDFs to publicly disclose how algorithms process personal data or whether user consent is factored into automated decision-making. This creates a loophole

		in algorithmic accountability, particularly for platforms involved in personalised advertising, credit scoring, and algorithmic content recommendations. The regulation should mandate that SDFs publish periodic reports on algorithmic transparency, detailing: (a) how personal data is used in decision-making, (b) whether user consent is considered, and (c) steps taken to prevent unfair biases or discriminatory outcomes. Additionally, there should be explicit obligations to ensure that AI-driven pricing, recommendations, or profiling do not violate consumer rights, enable anti-competitive practices, or engage in price discrimination. These measures align with DPDP Act, 2023 – Section 8 (Obligations of Data Fiduciaries) and Consumer Protection Act, 2019 (Prevention of Unfair Trade Practices).
12	**Rule 13** Rights of Data Principals	Rule 13 should ensure that Data Principals can review and withdraw consent easily, without unnecessary obstacles such as hidden cancellation buttons, multi-step processes, or requiring direct contact with customer support. Any "Subscription Traps" or consent withdrawal barriers should be explicitly classified as violations under the Act, aligning with the Guidelines for Prevention of Dark Patterns, 2023. Platforms should be required to implement a single-toggle consent revocation mechanism that is easily accessible and complies with DPDP Act, 2023 – Section 6 (Ease of Consent Withdrawal). Users should have clear rights regarding AI-driven pricing decisions, ensuring that they are: (a) Informed if AI-driven personalised pricing is applied to them, (b) Able to opt out of personalised pricing and choose a standard, non-personalised fixed price, and (c) Allowed to contest AI-based pricing decisions and request a human review if they believe the pricing was unfair. This aligns with DPDP Act, 2023 – Section 6 (Consent Mechanisms), Section 13 (User Rights), and the Consumer Protection Act, 2019 (Price Transparency Mandate). The regulation should prevent platforms from exploiting behavioural data for discriminatory pricing and require transparency in algorithmic pricing decisions, ensuring that consumers are not misled by opaque or unfair AI-driven pricing practices.
13	**Rule 15** Exemption from Act for research, archiving or statistical purposes.	**Lack of User Opt-Out, Privacy Safeguards & Clarity on Research Exemptions:** Rule 15 grants broad exemptions for research, archiving, and statistical purposes without providing Data Principals the right to opt out of having their personal data used for such purposes. Additionally, the rule does not establish clear safeguards on how research data should be processed, stored, or anonymized, increasing the risk of data misuse or re-identification. The language around the research exemption needs to be clarified to explicitly state that research should serve the public interest and must not be used as a loophole for private corporations to obtain data. The exemption should be strictly limited by the purpose limitation principle to prevent potential abuse.
14	**Rule 15**	Research exemptions should not relieve Data Fiduciaries from the duty of safeguarding user privacy. Yet, Rule 15 is not prescriptive on anonymisation methods like pseudonymisation, differential privacy, or encryption before use for research purposes. The language around the research exemption needs to be clarified to explicitly state that research should serve the public interest and

		must not be used as a loophole for private corporations to obtain data. The exemption should be strictly limited by the purpose limitation principle to prevent potential abuse.