INDIAN GOVERNANCE AND POLICY PROJECT

INDIAN GOVERNANCE AND POLICY PROJECT

COMMENTS TO THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY ON THE DRAFT DIGITAL PERSONAL DATA PROTECTION RULES, 2025

Authored by
Dedipyaman Shukla / Jhanvi Anam

relations@igap.in | igap.in

SUMMARY OF RECOMMENDATIONS

1 Clear Compliance Timelines

Establish phased and explicit deadlines for compliance with various provisions of the DPDP Act and Draft Rules.

2 Guidance on Notices

Define a reasonable 'look-back' period and clarify language requirements for all data processing notices.

3 Clarifying Precise Information Security Standards

Replace vague phrases such as 'at the minimum' with 'where appropriate' and align the information security safeguards with internationally recognized standards.

4 Risk-Based and Practical Data Breach Intimation

Introduce clear thresholds for the intimation of personal data breaches, adopting a conditional risk-based approach. Extend the current 72-hour intimation window for Data Principals.

5 Effective Consent Verification

For obtaining parental/guardian consent for children and persons with disabilities, adopt an 'actual knowledge' standard, and encourage innovative identity verification techniques.

6 Modified Exemptions for Children Data Processing that Promote Online Safety

Allow broader purpose-based exemptions for tracking and behavioural monitoring that protect children's online safety, coupled with a clear definition or illustration of what constitutes a 'detrimental effect.'

7 Clarified Cross-Border Data Transfer Rules

Articulate a clear distinction between conditions imposed on data transfers and outright restrictions. The language should align with Section 16 of the DPDP Act by focusing on restrictions based on territories or countries rather than on persons or entities.

8 Refined Information Request Protocols

Clarify confidentiality and non-disclosure requirements related to data requests under Rule 22. Additionally, specify whether decryption is expected, and limit the scope of information sought for classifying an entity as an SDF to ensure proportionality and safeguard privacy.

PRELIMINARY COMMENTS

The Indian Governance and Policy Project ***(IGAP)*** is a premier think-tank dedicated to fostering technological growth, innovation and development with a clear focus on addressing people's needs. Established to address the pressing challenges of policy implementation and institutional governance, IGAP collaborates with various stakeholders, including government bodies, academic institutions, and civil society organizations. Our mission is to foster informed policymaking through rigorous research, expert analysis, and stakeholder engagement. We envision a future where technological progress drives societal advancement across all strata.

At the outset, we welcome the multiple opportunities which the union Ministry of Electronics and Information Technology ***(MeitY)*** has provided to Indian stakeholders to submit their comments and suggestions on the country's new data protection framework, which includes the Digital Personal Data Protection Act, 2023 ***(DPDP Act)*** and the recently released Draft Digital Personal Data Protection Rules, 2025 ***(Draft Rules)***.

These consultative initiatives are indicative of the commitment of MEITY towards ensuring that a robust, effective and balanced legal framework is created to cater to the needs of Digital India. They also demonstrate the commitment of the Central Government towards implementing the spirit of the Pre-legislative Consultative Policy.[1]

Our suggestions for the Draft Rules, specified below, aim to strengthen the balance between the individual's constitutional Right to Privacy (as reiterated by the Supreme Court in *Justice K. S. Puttaswamy (Retd.) v. Union of India*[2]) and the needs of Data Fiduciaries to lawfully process personal data and provide a high standard of services to the public.

ISSUES AND RECOMMENDATIONS

1 Clarity on Date of Enforcement under Rule 1

Under Section 1(2) of the DPDP Act, discretion is provided to the Central Government to determine the date of enforcement. This includes the flexibility to designate different dates for different provisions of the Act (i.e. phased implementation). In this regard, it should be noted that over 1.5 years have elapsed since the law's enactment in August 2023.

While preliminary comments from MeitY representatives indicate that a maximum of 2 years may be provided for entities to transition to the new data protection regime, it would be beneficial to prescribe within the DPDP Rules clear compliance timelines for the multitude of its provisions.[3]

Clear timelines provide businesses and societal stakeholders with a structured roadmap for compliance, reducing ambiguity about when specific obligations may take effect. This clarity will help with planning and internal resource allocation within organizations expecting to be regulated as Data Fiduciaries.

Precedent for such timelines is also available in the context of previous privacy legislation. Some elements of the European Union's General Data Protection Regulation ***(GDPR)*** such as the 'Data Protection Directive for the police and justice sectors' were made applicable 2 years after the enactment of the law.[4]

RECOMMENDATION

To enhance DPDP Act enforcement clarity, MeitY may consider **a phased, but explicit, compliance timeline** for the DPDP Act and Draft Rules, **while accommodating sector specific considerations.** These timelines may clearly outline when the enforcement of penalties or regulatory actions will commence to ensure predictability, and prevent arbitrary enforcement.

2 Enhanced Guidance on Notice Provisions under Rule 3

Section 5 of the DPDP Act mandates that a notice must be provided to the Data Principal in line with Section 5 prior to a request for consent for processing of any personal data. Notices are also required for personal data already being processed, based on consent, prior to the DPDP Act's enforcement. Rule 3 specifies some minimum requirements in this regard, which include – (i) an itemised description of personal data; and the specified purpose of, and (ii) a description of the goods or services to be provided or uses to be enabled by, such processing.

While this guidance on issuing notice is notable, some concerns with the practical implementation of personal data notices remain.

a *'Lookback Period' for Data Processing*

While Data Fiduciaries are required to give notice to Data Principals regarding previous processing as soon as it is reasonably practicable, the rules do not identify the 'look-back' period for such notices.

Retrospective notices to all data principals, regardless of the vintage of the personal data, may prove to be resource-intensive, and may require restructuring existing data processing activities. Further, data of significant vintage may create operational challenges in issuing notices, due to changes in contact information which may have taken place in the several years leading up to enforcement.

b *Notice for Previous Consent*

The requirement under Section 5(2) of the DPDP Act may also be misaligned with the existing privacy framework under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ***(SPDI Rules)***, forcing further segregation of legacy personal data. These SPDI Rules (under Rule 5) mandate notices for sensitive personal data or information, and not all personal data processed by a body corporate.

Consequently, some form of 'consent' may not have been provided for all personal data previously under the SPDI rules. Section 5(2) of the DPDP Act mandates the identification of data for look-back notices, for which consent has been provided. The contrast between these provisions is not clarified within the DPDP Rules.

c *Language of Notice*

Section 5(3) of the DPDP Act provides that the contents of a notice must be accessible in 'English or any language specified in the Eighth Schedule to the Constitution'. The phrasing of this provision creates an additional ambiguity in the context of India's linguistic and regional diversity.

It is not clear whether the requirement implies that the notice for consent must be in - (i) English and any 1 additional language under the Eighth Schedule, (ii) The notice must provide the option to be 'translated' to any language under the Eighth Schedule, or (iii) The notice must be intelligible in the Eight Schedule language relevant to the user. In this respect, the Draft Rules, merely prescribe that such notice must be provided 'in clear and plain language.'

d *Dark Patterns in Notices*

Although clarity is stressed in the Draft Rules, the requirement for itemized data and uses does not exclude the potential for abuse through dark patterns which exploit consent fatigue, as well as the behavioural proclivities of users. For instance, an itemized description of personal data could still be presented in a lengthy format, forcing users to click through multiple checkboxes to give their consent.

A 'select all' checkbox that automatically opts users into all data uses could subtly coerce Data Principals into giving blanket consent without fully understanding the implications. These dark patterns in seeking consent could undermine the intent of the Draft Rules by manipulating Data Principals into consenting in ways that are neither informed, nor voluntary.

RECOMMENDATION

To ensure that the degree of guidance on notices is adequate yet balanced, the following may be incorporated into the Draft Rules

a. **A reasonable** and **defined look-back timeframe** for providing notices in relation to Section 5(2) of the DPDP Act, to data principals may be prescribed under the Draft Rules. For example, the Draft Rules may require that Data Fiduciaries may limit notices under Section 5(2) for existing personal data processing activities to data collected within the previous 3 years preceding the enforcement of the DPDP Act, utilizing available contact information.

b. Clarification may also be provided on the applicability of Section 5(2) notices to **all legacy personal data** within the defined timeframe, **whether or not it is identified as sensitive personal data or information under the SPDI Rules.**

c. **Language related clarifications** within the Draft Rules may also be provided to ensure **that notices remain intelligible to users,** in line with the principle of 'free and fair consent'.

d. Further, while the Draft Rules do not specify mechanisms to avoid dark patterns in notices, scope may be provided within the Draft Rules **to encourage the development of industry codes of practice on consent notices,** which are aligned with global best practices.[5]

3 Greater Clarity on Information Security Standards under Rule 6

The Draft Rules, while introducing guidance on reasonable security standards, indicate a shift from the established global standards of information security, such as the ISO/IEC 27000 series encouraged under the Information Technology Act, 2000.

While this shift in approach aims to enhance flexibility, it results in substantial ambiguity regarding the expectations from entities in maintaining a level of 'reasonable security'. Rule 6 mandates a range of activities (encryption, access controls, monitoring logs, data backups etc.) to be undertaken by Data Fiduciaries processing personal data.

These requirements are prefixed with the phrase 'at the minimum', implying that each security measures must be undertaken in all situations, for all personal data- types. Such a requirement does not address the appropriateness of the information security activity in relation to the nature of processing which a Data Fiduciary may undertake.

This requirement also risks imposing unnecessary operational measures on Data Fiduciaries, which may result in unnecessary limitations and a greater allocation of resources without the benefit of meaningfully increasing the level of security for Data Principals.

Further, the Draft Rules do not establish whether these new safeguards offer a higher or lesser level of security as compared to globally recognized ISO standards.

Unlike the Draft Rules, international standards like ISO 27000 outline a precise, objective and detailed set of technical requirements that are easy to measure and audit.

Without these 'benchmarks', organizations may face difficulty in demonstrating that they are compliant. Each business might interpret the requirements differently, leading to inconsistent practices and uncertainty. This can prove to be a concern during organizational due-diligence exercises, or legal scrutiny.

It should also be noted that the ambiguity in compliance with reasonable security expectations exposes significant risks for Data Fiduciaries operating in India. The Data Protection Board is empowered to impose fines of up to INR 250 crore for a breach in obligation to take reasonable security safeguards to prevent personal data
breach Section 8(5).

RECOMMENDATION

To ensure ease of understanding of expectations for under the DPDP Act, the phrase **'at the minimum'** in Rule 6 may be **replaced** with **'where appropriate'**. Further the Draft Rule's standard of reasonable security may be **'benchmarked' or equated to international standards** for information security, such as such as IS/ISO/IEC 27001.

4 Reasonable Intimation Thresholds of Personal Data Breaches under Rule 7

The framework of the DPDP Act rightly identified the intimation of personal data breaches as crucial to safeguarding the rights of Data Principals. However, the nature of breach-related obligations under the Draft Rules present operational challenges which may not be in the best interest of privacy protections for Indians.

The reporting of breaches in India remains an onerous activity with strong disincentives in place. These hurdles are unlikely to abate post the enforcement of the DPDP Act, and may become enhanced.

Based on an empirical evaluation, by IGAP, of data breach incidents taking place in India, the following concerns were identified:[6]

a. Data breach reporting places an extremely heavy resource burden on Data Fiduciaries which includes manpower for cyber security, identification and outreach to affected Data Principals, and regulatory costs for engaging with authorities.

b. Reporting of breaches which amount to a public disclosure can also have a significant impact on the brand value and share price of private entities after each reporting. This could require additional public-relations management resources.

c. Levels of incident disclosures remain far below the estimated number of personal data breaches occurring in India annually.

The DPDP Act does not provide an threshold for the reporting of data breaches, despite their diverse types and varying severities. Each breach incident is required to be intimated to the Data Protection Board and each affected principle. This approaches diverges from many other jurisdictions, such as the European Union, Singapore, and Japan where intimation is conditional upon the significance of the harm from the breach.[7]

Additionally, we note that the compliance period of 72 hours for intimating possibly millions of data principals, in each instance, is prescribed. A report of the same is required to be submitted to the Board.

In relation to the scale of thisrequirement, the timeline provided is very short. Short reporting deadlines may make it challenging for MSMEs and other smaller Data Fiduciaries, which carry limited operational capacity, to provide the granular information as required by the Data Protection Board and affected persons. These cumulative factors could lead to substantial operational strain on Data Fiduciaries, and re-enforce the disincentives against breach intimation.

Further, the lack of intimation thresholds risk a complete inundation of the regulatory authority (Data Protection Board), and consequent 'breach fatigue' in case of Data Principals. With high volumes of breaches, the Board may struggle to identify and prioritize high-impact breaches for corrective or mitigatory action. Further, constant intimations to users about even minor breaches may de-sensitize Data Fiduciaries about risks, leading to breach fatigue, and diminish their willingness to take precautionary actions.

RECOMMENDATION

To preserve the effectiveness and utility of personal data breach intimations, the Draft Rules may incorporate **clear thresholds for intimation,** which utilize a conditional **'risk-based approach'.** Breaches that do not pose a high risk to individual rights and freedoms, should only require a minimalist and simplified intimation format.

Further, the **timeline for intimation of Data Principals** in necessary cases may be **extended beyond the current 72-hour window** to reduce operational constraints on small organizations.

5 Functional Approaches to Obtaining Verifiable Consent for Child/Person with Disability under Rule 10

The DPDP Act requires that the verifiable consent of the parent or lawful guardian must be obtained before processing any personal data of a child or a person with disability. Rule 10 of the Draft Rules further provides that a Data Fiduciary shall adopt appropriate technical and organisational measures are taken to ensure that verifiable consent of the parent is obtained before processing of any personal data of a child.

Potentially implicit in this consent requirement is the need for Data Fiduciaries to know in which cases is the parental/guardian's consent is necessary (i.e. that the Data Principal is below 18 years of age, or has a disability).

This standard cannot be reliably implemented without age-gating the entire platform of a Data Fiduciary, and effectively making some form of Know-Your-Customer ***(KYC)*** obligations the norm for most digital services and activities taking place digitally. Implementing such a system is expected to be a resource intensive process, which may involve developing new secure systems, and integration with third-party services.

While large entities may be able to absorb these costs, the impact on India's start-up ecosystem and estimated 6.3 crore MSMEs[8] may be significant due to the diversion of limited resources and personnel towards compliance.

The following specific concerns in relation to Parent and Guardian verification should also be noted:

a *Verifiable Parental Consent*

Rule 10 of the Draft Rules prioritizes Government-issued identification or mapped virtual tokens as the means for verification of identity. The provision also references Digital Locker services providers.

Integration with Government-based identification (such as the Unique Identification Authority of India ***(UIDAI)***'s Aadhaar e-KYC API) involves the setup of technical infrastructure. Further, in September 2021, UIDAI released the draft Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021, which specified a cost of INR 3 for each e-KYC transaction and INR 0.50 for each 'Yes/No' authentication transaction.[9] Recent estimations by CUTS International of the cost of implementing verifiable parental consent in other countries indicate at a USD 35,000 cost in developing infrastructure, and USD 70,000-120,000 in ongoing annual costs.[10]

The utilization of these mechanisms which would add additional cost burdens to the limited resources available to MSMEs. The feasibility of passing these costs to users would also be limited in multiple cases, as digital businesses in India often thrive on a low-level of friction at the stage of user registration, and a comparatively low Average Revenue Per User ***(ARPU)***.[11]

b *Consent of Guardians of Persons with Disabilities*

As per Rule 10, a unique requirement is placed on Data Fiduciaries to observe a 'due diligence' to verify that a guardian of a person with disability is appointed by a court of law, a designated authority or a local level committee. As compared to the process for children, this requirement introduces

greater complications and suggests that entities would need to authenticate official court orders or legal documentation. At present, India does not provide a centralized system, which is digitally accessible, for verifying guardianship orders.

The Draft Rules themselves list multiple laws for validating disabilities including the Rights of Persons with Disabilities Act, 2016 and the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999. Developing systems for validation of potentially physical and non-standardized documents issued by different courts under different laws would be a significant exercise regardless of the size or sector of a Data Fiduciary. Further, this requirement would extend to entities that do not cater specialized services to either children, or persons with disabilities.

Additionally, the approach of the DPDP Act and Draft Rules towards persons with disabilities takes a rigid stance (regardless of the wide diversity of diagnosed disabilities) on the incapacity of such persons to make binding decision on personal data processing. This contradicts the intent established by the Supreme Court in its decision in Rajive Raturi v. Union of India (2024)[12], where it noted the principle of 'universal design' in making all services usable by individuals with disabilities to the greatest extent possible to prevent their marginalization.

RECOMMENDATION

To preserve the interests of vulnerable groups like children and persons with disabilities, while balancing operational constraints in the digital space, the Draft rules may incorporate an **'actual knowledge'** based standard for verifiable parental consent requirements, as well as guardian-related consent for persons with disabilities. Further, the requirement to obtain guardian's consent for persons with disabilities may be restricted to such instances where there is **'apparent incapacity'**, which preserves the access of most individuals to digital services.

Additionally, the Draft Rules may **encourage** the adoption of more **flexible verification solutions** for parent/guardian consent, such as age-estimation, video, or 'social vouching' (relying a user's community to vouch for their identity credentials).

6 Expanded Exemptions from Certain Restrictions for Processing Children's Data under Rule 11

The Draft Rules exempt classes of Data Fiduciaries from processing restrictions. In particular the restrictions on Data Fiduciaries to not undertake tracking or behavioural monitoring of children is exempted for entities such as educational institutions, crèches, child care centres, and mental health establishments. Certain purposes are also exempted, including the blocking of access of a child to information which may have a detrimental effect on wellbeing. However, mere blocking of access does not sufficiently cover the extent of use of modern online safety mechanisms.

As observed by the Supreme Court in *Justice K. S. Puttaswamy (Retd.) v. Union of India*[13], children are remain vulnerable in digital spaces and should not face lifelong consequences for their naive digital behaviours. Aligning with this school of thought, many platforms deploy online-safety technologies that protect against real- world harms caused by digital interactions, such as 'text classification systems' to detect predatory behaviour/grooming,[14] and artificial intelligence driven 'hybrid deep learning approaches' to detect cyberbullying.[15] The mechanism of such systems often involve the tracking monitoring of online user activity, mere flagging, and content classification without immediately preventing 'access to information'. While such technologies and systems demonstrably enhance user safety, they may not precisely align with the limited exemptions under Rule 11.

In connection with this, the DPDP Act's prohibition on processing that may have a 'detrimental effect on the well-being of a child', under Section 9(2) lacks clarity. Although the phrase is also used under the Draft Rules, no guidance or illustration is provided on what amounts to a detrimental effect.

In the absence of this guidance, Data Fiduciaries may struggle to anticipate intangible detriments, such as behavioural or psychological impacts, of their data processing in relation to children. In an earlier iterations of the draft law, a related concept of 'harm' in relation to Data Principals was defined under Clause 2(10) to include bodily harm, identity theft, harassment, and significant loss.[16]

RECOMMENDATION

The Draft Rules may allow for a **broader purpose-based exemption** for tracking and behavioural monitoring that serve beneficial functions in the interest of online safety without creating risks of harm. Such an exemption should **enable data processing by a Data Fiduciary which mitigates a 'detrimental effect' on a child.**

Further, a clear and specific **definition or illustration** may be incorporated within the Draft Rules for **'detrimental effect'** in relation to children to reliably guide
personal data processing.

7 Processing of Personal Data Outside India under Rule 14

Section 16 of the DPDP Act enables the Central Government to restrict the transfer of personal data by a DF for processing to such country or territory outside India as may be so notified. Through this provision a 'blacklist' approach has been adopted where cross-border data transfers are allowed, However, the Draft Rules provide further conditions in that a Data Fiduciary 'shall meet such requirements as the Central Government may…specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.'

The phrasing of this provision suggest restricting transfers to Governments (i.e. specific entities) rather than specific regions creating a notable dissonance between the language of the DPDP Act and the Draft Rules.

The Draft Rules also do not clarify if, and how, sector specific personal data transfers may be restricted under Rule 14. As per public statements by the Hon'ble Union Minister for MeitY,[17] a government- appointed committee may evaluate localization needs raised by sectoral ministries. To illustrate this issue, if a government-appointed committee determines that certain categories of 'health data' should be subject to localization, it is unclear if such restrictions could be operationalized under the Draft Rules.

RECOMMENDATION

Rule 14 may articulate a **clear distinction between the 'conditions on transfer'** and 'restricting transfer' of personal data may be necessary to provide clarity and ensure enforceability without creating undue burdens on stakeholders. Further, the Draft Rules may **incorporate language reflecting restrictions** on transfers to **'territories' or 'countries', as opposed to 'persons' or 'entities',** in alignment with Section 16 of the DPDP Act.

8 Modifications to Calling for Information from Data Fiduciaries or Intermediaries under Rule 22

Rule 22 allows the Central Government to call for furnishing such information held by Data Fiduciaries or intermediary for reasons, which includes the interests of State Sovereignty, integrity, and security as well as legal enforcement purposes. The rule also enables authorized persons to direct non-disclosure in respect of the order as well.

However, the phrasing of this provision creates an ambiguity in terms of where the confidentiality expectations may be applicable (i.e. whether it applies in relation to the disclosure of the request for information, or public disclosure of the information itself). Under the present Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (***LIM Rules)***, which enable interceptions under Section 69 of the IT Act, intermediaries are required to maintain secrecy and confidentiality in relation to interception, monitoring and decryption. Similar clarity on the expectations under the Draft Rules are not present. It is also unclear whether Rule 22 carries an expectation for entities to 'decrypt' requested information, similar to Section 69 of the IT Act. Rule 6 of the Draft Rules mandates the securing of personal data through its encryption.

It is also worth noting that compared to past precedents, such as Rule 419A of the Indian Telegraph Rules, 1951 (under the Indian Telegraph Act, 1885) and the LIM Rules, the Draft Rules do not provide a similar standard of safeguards in case of information requests. For these earlier frameworks, oversight is carried out through a Review Committee set up under the Rule 419A (16) of the Telegraph Rules. Both of these interception frameworks clearly identify the minimum rank of officers authorized to exercise such powers ,and the extraordinary circumstances under which such actions may be taken. Rule 22, however, does not provide clear criteria for designating authorized persons, nor does it specify the ranks of such officers.

Finally, Rule 22 conflates similar information requirements and procedures for (i) highly sensitive national security purposes, and (ii) designation of any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary ***(SDF)***.

At the outset, it is unclear if requesting of personal data would be necessary for the purpose of SDF classification. Further, the extent of such blanket empowerment may, in the future, enable information requests, which do not meet elements of the standard of 'proportionality' outlined by the plurality of opinions in *Justice K. S. Puttaswamy (Retd.) v. Union of India*[18], and articulated by Justice Kaul.

For context, the judgement noted that an interference of the fundamental right to privacy would require, among other things, (i) justification that the extent of interference was proportionate to its need, and (ii) presence of procedural guarantees against abuse of the interference.[19]

As noted above, the wide mandate of the designated officer in MEITY to request information for the classification of SDF is equivalent to the mandate of designated officers in national security cases, which may carry far more significant ramifications. Further, this power is not curtailed in terms of the data requirements relevant to assessing the characteristics of Data Fiduciaries. Additionally, no additional safeguards for information requests (akin to those under the LIM Rules and Telegraph Rules) is provided.

RECOMMENDATION

To ensure existing standards of interception and information requests are adhered to, the following elements may be incorporated within Rule 22:

a **Clarification on confidentiality or non-disclosure expectations** from Data Fiduciaries in relation to calls for information, in line with the previous LIM Rules.

b **Clarification on the expectation to decrypt data** in response to information requests.

c **Additional conditions and personal data-related safeguards** specific to the **purpose of calling information to designate an entity as an SDF.** These conditions may restrict the power of the designated officer to 'information- types' relevant to the classification exercise (for example, this may include (i) aggregate information on personal data volumes processed, (ii) types of data processed, (iii) compliance track record, (iv) breadth of operations, and (v) metrics outlining potential harms to the privacy of individuals).

FOOTNOTES

1 Pre-legislative Consultation Policy (PCLP), 5 February 2014, available at https://cdnbbsr.s3waas.gov.in/s380537a945c7aaa788ccfcdf1b99b5d8f/uploads/2023/02/2023021333.pdf.

2 Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCR 569.

3 Information available at https://www.thehindu.com/sci-tech/technology/it-minister-ashwini-vaishnaw-on-digital-personal-data-protection-rules-2025/article69077503.ece.

4 Legislative History of GDPR, available at https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

5 Example of European Guidance on Dark-Patterns, available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

6 IGAP Report: Anticipating Compliance with the Digital Personal Data Protection Act, 2023 on Data Breaches in India (November 2024), available at https://www.igap.in/anticipating-compliance-with-the-digital-personal-data-protection-act-2023-on-data-breaches-in-india-2.

7 Data collected from country specific laws, as well as the DLA Piper Data Protection Laws of the World database, available at https://www.dlapiperdataprotection.com.

8 Annual Report 2023-24, Ministry of Micro, Small and Medium Enterprises, available at https://msme.gov.in/sites/default/files/FINALMSMEANNUALREPORT2023-24ENGLISH.pdf.

9 Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021, available at https://uidai.gov.in/images/Draft_Auth_Pricing_Regulations.pdf.

10 Economic Analysis of Verifiable Parental Consent Mechanisms: Evaluating Impact on Consumers and Data Fiduciaries, CUTS International, February 2025, available at https://cuts-ccier.org/pdf/economic-analysis-of-verifiable-parental-consent-mechanisms-evaluating-impact-on-consumers-and-data-fiduciaries.pdf

11 For instance, in the telecom sector, which is one of the most used and vital services in India with 1.15 billion wireless subscribers, the monthly APRU for wireless services is merely INR 172.57 or approximately USD 1.98, as of January 2025, Available at https://www.trai.gov.in/sites/default/files/2025-01/QPIR_01012025_0.pdf.

12 Writ Petition (c) No. 228/2006.

13 Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCR 569.

14 A. Faraz, J. Mounsef, A. Raza and S. Willis, "Child Safety and Protection in the Online Gaming Ecosystem", in *IEEE* Access, vol. 10, pp. 115895-115913, 2022, available at https://ieeexplore.ieee.org/document/9933399.

15 B. A. H. Murshed, J. Abawajy, S. Mallappa, M. A. N. Saif and H. D. E. Al-Ariki, "DEA-RNN: A Hybrid Deep Learning Approach for Cyberbullying Detection in Twitter Social Media Platform," in *IEEE* Access, vol. 10, pp. 25857-25871, 2022, available at https://ieeexplore.ieee.org/document/9718597.

16 Draft Digital Personal Data Protection Bill, 2022, available at https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022.

17 Report available at https://www.financialexpress.com/life/technology-sectoral-needs-to-drive-data-localisation-restrictions-to-be-applied-only-where-needed-govt-3707437/lite/.

18 Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCR 569.

19 Paragraph 71, *Justice Sanjay Kishan Kaul, Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCR 992.*

INDIAN
GOVERNANCE AND
POLICY PROJECT

IGAP INDIAN GOVERNANCE AND POLICY PROJECT

The Indian Governance And Policy Project (IGAP) is an emerging think tank focused on driving growth, innovation, and development in India's digital landscape. Specializing in areas like AI, Data Protection, FinTech, and Sustainability, IGAP promotes evidence-based policymaking through interdisciplinary research. By working closely with industry bodies in the digital sector, IGAP provides valuable insights and supports informed decision-making. Core work streams include policy monitoring, knowledge dissemination, capacity development, dialogue and collaboration.

For more details visit: www.igap.in

relations@igap.in | igap.in