IGAP INDIAN GOVERNANCE AND POLICY PROJECT

From Law to Action

The Digital Personal Data Protection Act and Rules: Overview and Key Implications

FROM LAW TO ACTION THE DIGITAL PERSONAL DATA PROTECTION ACT AND RULES: OVERVIEW AND KEY IMPLICATIONS

November 2025

Published by
Indian Governance and Policy Project (IGAP)

Authored by
Shachi Solanki and Ananya Agrawal

Edited by
Dedipyaman Shukla

Designer
Manoj Murali

About IGAP
The Indian Governance and Policy Project (IGAP) is a policy, business advisory, and research studio working at the intersection of governance, technology, markets, and national development.

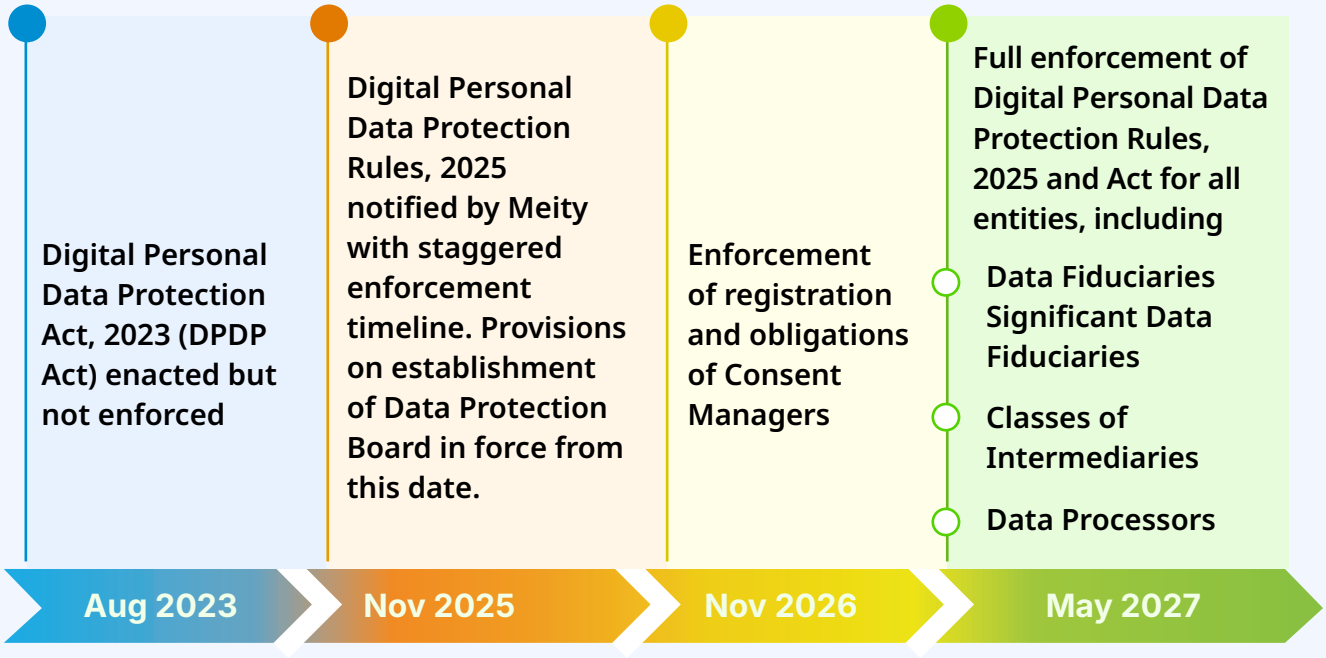
Grounded in a clear understanding of how state capacity, market forces, and emerging technologies shape India's strategic trajectory, IGAP addresses key questions that define the country's future — from the governance of AI and digital infrastructure to financial innovation, sustainability, and national security.

Bringing together lawyers, policy thinkers, and strategists with deep business and geopolitical insight, IGAP delivers solutions that balance India's developmental and security priorities with its democratic values and constitutional principles.

Introduction

On November 13, 2025, the Ministry of Electronics and Information Technology (MeitY) notified the Digital Personal Data Protection Rules, 2025, marking a pivotal milestone in India's data governance journey by operationalizing the Digital Personal Data Protection Act, 2023. These Rules translate the Act's statutory framework into actionable compliance obligations, establishing a phased implementation timeline spanning 18 months to enable organizations to build requisite institutional capacity, technical infrastructure, and operational safeguards. The notification follows extensive public consultation, incorporating stakeholder feedback and introducing several changes. The Rules establish India's first comprehensive privacy regulatory regime, balancing individual privacy rights with legitimate state interests, business operational flexibility, and digital economy growth imperatives. This analysis examines the implementation roadmap, comparative changes from Draft to Final Rules, and compliance implications for entities navigating India's evolving data protection landscape.

Implementation Timeline:
Digital Data Protection Act, 2023 and Rules, 2025



Compliance Roadmap and Operational Impact

Phase I: Immediate Effect

Constitution of Data Protection Board (DPB)

The DPB of India will function as a quasi-judicial body for privacy enforcement, inquiring into breaches reported by citizens or detected through breach notifications, issuing corrective directions to organizations, and imposing financial penalties up to INR 250 crore for violations of data protection obligations.

The establishment of the DPB may start immediately. A search-cum-selection committee appointed by the Central Government will appoint the chairperson and members of the DPB.

After the 18-month implementation period, the DPB will undertake its regulatory and adjudicatory functions to protect individual privacy rights.

Phase II: 1 Year From Notification

Consent Management Framework

1 year from the notification of the rules, the registration process for consent managers with the DPB will begin. Consent Managers will be entities that enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

To be registered by the DPB, entities must fulfill the eligibility conditions set out in Part A of the First Schedule, including incorporation in India, minimum net worth of INR 2 crore, sound financial standing, and independent certification of platform interoperability, and technical and organisational safeguards.

Phase III: 18 Months from Notification

Operational Compliance

Phase III operationalises the full suite of obligations under the DPDP Act and Rules. The key compliance requirements are outlined below.

Lawful Basis of Processing: Entities must map each processing activity to one of the legitimate grounds available under the Act, which can be broadly categorised as:

- Consent-based processing
- Voluntary provision without objection
- State functions including subsidies, benefits, public services, legal obligations, and court orders
- Medical emergencies and public health interventions
- Safety, assistance and services during disasters or breakdown of public order
- Employment related purposes

Notice Requirement: Data Fiduciaries must provide clear notices that specify the personal data collected and its corresponding purpose of processing. Every consent request must be supported by a clear and plain notice outlining the data, purpose(s), and means for withdrawal of consent, exercise of rights, and filing complaints.

User Rights and Safeguards: Data fiduciaries must enable user rights to access, correct, update and erase their personal data. Grievance redressal mechanisms should be in place with processes to address complaints within 90 days, exhausting which Data Principals may escalate them to the DPB.

Data Breach Reporting: Data Fiduciaries must notify affected Data Principals immediately and "without delay" upon becoming aware of any personal data breach, providing concise, clear descriptions of the breach nature, consequences, mitigating measures, and safety precautions users should take. They have to parallely report to the DPB, first providing an initial breach intimation without delay, followed by detailed incident reports within 72 hours (or longer if approved by the DPB). Failure to report breaches carries penalties up to INR 200 crore.

Children's Data and Special Protections: Children's data can only be processed after obtaining verifiable parental consent. Additional safeguards must be implemented to protect children's data online and safeguard them from tracking, monitoring, and targeted advertisements. The Rules carve out narrow, purpose-bound exemptions from these requirements for specific classes of Data Fiduciaries when processing is strictly necessary for health services, educational activities, or child safety. New purpose-based exemptions in the Final Rules permit real-time location tracking for child safety and expanded filtering of harmful information, services, or advertisements likely to cause detrimental effects on child well-being.

For persons with disabilities unable to take legally binding decisions, consent must be taken from lawful guardians verified by courts, designated authorities, or local level committees under applicable guardianship laws.

Significant Data Fiduciaries: Once notified by the Central Government based on data volume, sensitivity, and impact on sovereignty or democracy, Significant Data Fiduciaries must appoint India-based Data Protection Officers and independent auditors. They have additional compliance obligations under the DPDP Act, including annual data protection impact assessments, technological risk assessments, and compliance with government-specified data localization requirements for specified categories of data.

State Obligations: State entities processing personal data for public functions or research must ensure lawful and purpose-bound use, limit processing to what is necessary, maintain accuracy, completeness, consistency, apply appropriate retention practices, and implement suitable security measures. Where personal data is used to deliver public services or benefits, an intimation mechanism and clear avenues for exercising rights must also be provided.

Technical and Security Safeguards: Data Fiduciaries and their processors must implement encryption, access controls, continuous monitoring, and breach detection systems. Rule 6 lays down minimum safeguards, that can be structured into the following categories:

1. Data Protection Measures:

Encryption, obfuscation, masking, or virtual tokenization of personal data

2. Access and Monitoring Controls:

- Access controls restricting use of computer resources to authorized personnel
- Logging and monitoring systems to detect, investigate, and remediate unauthorized access
- Retention of logs and personal data for at least one year to enable breach detection and investigation

3. Business Continuity:

- Data backup measures ensuring continued processing if confidentiality, integrity, or availability is compromised

4. Contractual and Organizational Safeguards:

- Binding contractual provisions requiring Data Processors to implement equivalent security safeguards
- Appropriate technical and organizational measures ensuring effective observance of all prescribed safeguards

Data Retention: All Data Fiduciaries and their processors are required to maintain logs of personal data, traffic and processing for purposes of sovereignty, integrity, performance of any function under law, for a minimum period of one year. Specified entities with a large user-base, such as e-commerce, online gaming, and social media intermediaries have to maintain data logs for a minimum of three years.

Government Information Requests: The Central Government may require any Data Fiduciary or intermediary to furnish specified information for purposes including sovereignty, security, statutory functions, and assessment for Significant Data Fiduciary classification.

Cross-Border Data Transfers: The notified Rules adopt a negative-list approach wherein personal data may be transferred to any country unless explicitly restricted by Central Government notification. However, transfers to foreign States or entities under State control require compliance with government-specified requirements, targeting scenarios where foreign laws may compel data access. Organizations gain immediate cross-border transfer rights without advance government approvals, but must monitor government notifications blacklisting restricted jurisdictions.

Draft to Final Rules:
Key Changes and Compliance Implications

Short title and commencement Rule 1 of Final Rules		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) These rules may be called the Digital Personal Data Protection Rules, 2025. **(2)** Rules 3 to 15, rule 21 and rule 22 shall come into force with effect from _____. **(3)** These rules, except rules 3 to 15 and rules 21 and 22, shall come into force on the date of their publication in the Official Gazette.	**(1)** These rules may be called the Digital Personal Data Protection Rules, 2025. **(2)** Rules 1, 2 and 17 to 21 shall come into force on the date of their publication in the Official Gazette. **(3)** Rule 4 shall come into force one year after the date of publication of this Gazette. **(4)** Rules 3, 5 to 16, 22 and 23 shall come into force eighteen months after the date of publication of this Gazette.	**1. Three-tier implementation timeline:** **Immediately in force:** Rule 1: Short title and Commencement Rule 2: Definitions Rules 17-21: Establishment and Composition of the DPB **1 year from notification:** Rule 4: Registration and Obligations of the Consent Manager **18 Months from notification:** Rule 3: Notice Rules 5-16: Operational part of the Rules Rule 22: Appeal Rule 23: Calling for Information from Data Fiduciary or Intermediary **2. Phased implementation approach**: Institutional setup → consent infrastructure → comprehensive operational compliance: Entities have 18 months to comply with core obligations such as notice, breach notification, provision of user rights.

Definitions Rule 2 of Final Rules		
Draft Rules	**Final Rules**	**Implication of Changes**
Unless the context otherwise requires, all expressions shall have the meaning assigned to them in the Digital Personal Data Protection Act, 2023 (22 of 2023) (hereinafter referred to as "Act").	**(1)** In these rules, unless the context otherwise requires, (a) "Act" means the Digital Personal Data Protection Act, 2023 (22 of 2023); (b) "techno-legal measures" means as referred to under rules 20 and 22; (c) "user account" means the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such Data Principal is able to access the services of such Data Fiduciary; and (d) "verifiable consent" means a consent as specified in rule 10 or 11. **(2)** The words and expressions used in these rules and not defined, but defined in the Act, shall have the same meanings respectively assigned to them in the Act.	**New definitions added:** **1. "Techno-legal measures":** The Final Rules introduce this term in the definition clause, cross-referencing it to Rules 20 and 22 on the digital office functioning of the DPB and the Appellate Tribunal. Both these bodies may adopt "techno-legal measures" to conduct proceedings in a manner that does not require the physical presence of any individual. The term lacks substantive definition, where neither Rule 2(1)(b) nor the referenced Rules 20 and 22 specify what these measures entail, creating a circular reference. **2. "User account":** Previously defined separately in Rules 7(3) and 8(3) of the Draft Rules, the Final Rules consolidate this in the definition clause for uniform application across all rules. **3. "Verifiable consent":** The Final Rules introduce this definition, cross-referencing Rules 10 and 11 which establish the process for obtaining consent for processing personal data of children and persons with disabilities.

Notice by Data Fiduciary Rule 3 of Final Rules (Under S. 5 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
The notice given by the Data Fiduciary to the Data Principal shall— **(a)** be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary; **(b)** give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum,— (i) an itemised description of such personal data; and (ii) the specified purpose of, and an ~~itemised~~ description of the goods or services to be provided or uses to be enabled by, such processing; and **(c)** the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may— (i) withdraw her consent, with the ease of doing so being comparable to that with which such consent was given; (ii) exercise her rights under the Act; and (iii) make a complaint to the Board.	The notice given by the Data Fiduciary to the Data Principal shall— **(a)** be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary; **(b)** give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum, — (i) an itemised description of such personal data; and (ii) the specified purpose or purposes of, and specific description of the goods or services to be provided or uses to be enabled by, such processing; and **(c)** give, the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may— (i) withdraw her consent, with the ease of doing so being comparable to that with which such consent was given; (ii) exercise her rights under the Act; and (iii) make a complaint to the Board.	**1. "Itemised description" → "Specific description":** The Final Rules remove the requirement of providing itemised description of goods and services in notices. This shifts compliance focus from formalistic checklist presentation to substantive adequacy of information disclosure. **Notice design optimization:** This change simplifies compliance with notice requirements for Data Fiduciaries. It provides flexibility on notice formats and removes the requirement to map purposes of processing with itemized goods or services. **2. "Specified purpose" → "Specified purpose or purposes":** This change explicitly permits single consent covering multiple related purposes. This can enable upfront disclosure of interconnected functions without fragmented consent flows that degrade user experience. This is particularly relevant for certain sectors like the BFSI, where single customer data can serve multiple purposes including regulatory compliance, service delivery, risk assessment, and statutory reporting. **Specificity safeguard:** While permitting multi-purpose disclosure, Data Fiduciaries must ensure each purpose remains "specific" as per Section 6 of the Act and cannot use plural form to obtain blanket consent.

Registration and Obligations of Consent Manager Rule 4 + Schedule I of Final Rules (Under S. 6 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager by furnishing such particulars and such other information and documents as the Board may publish in this behalf on its website. **(2)** On receipt of such application, the Board may make such inquiry as it may deem fit to satisfy itself regarding fulfilment of the conditions set out in Part A of First Schedule, and if it— (a) is satisfied, register the applicant as a Consent Manager, under intimation to the applicant, and publish on its website the particulars of such Consent Manager; or (b) is not satisfied, reject the application and communicate the reasons for the rejection to the applicant. **(3)** The Consent Manager shall have obligations as specified in Part B of First Schedule. **(4)** If the Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations under this rule, it may, after giving an opportunity	**(1)** A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager by furnishing such particulars and such other information and documents as the Board may publish in this behalf on its website. **(2)** On receipt of such application, the Board may make such inquiry as it may deem fit to satisfy itself regarding fulfilment of the conditions set out in Part A of First Schedule, and if it— (a) is satisfied, register the applicant as a Consent Manager, under intimation to the applicant, and publish on its website the particulars of such Consent Manager; or (b) is not satisfied, reject the application and communicate the reasons for the rejection to the applicant. **(3)** The Consent Manager shall have obligations as specified in Part B of First Schedule. **(4)** If the Board is of the opinion that a Consent Manager is not adhering to the conditions and obligations under this rule,it may, after giving an opportunity of being heard, inform the Consent Manager of such nonadherence	No change

of being heard, inform the Consent Manager of such non-adherence and direct the Consent Manager to take measures to ensure adherence. **(5)** The Board may, if it is satisfied that it is necessary so to do in the interests of Data Principals, after giving the Consent Manager an opportunity of being heard, by order, for reasons to be recorded in writing,— (a) suspend or cancel the registration of such Consent Manager; and (b) give such directions as it may deem fit to that Consent Manager, to protect the interests of the Data Principals. **(6)** The Board may, for the purposes of this rule, require the Consent Manager to furnish such information as the Board may call for.	and direct the Consent Manager to take measures to ensure adherence. **(5)** The Board may, if it is satisfied that it is necessary so to do in the interests of Data Principals, after giving the Consent Manager an opportunity of being heard, by order, for reasons to be recorded in writing, — (a) suspend or cancel the registration of such Consent Manager; and (b) give such directions as it may deem fit to that Consent Manager, to protect the interests of the Data Principals. **(6)** The Board may, for the purposes of this rule, require the Consent Manager to furnish such information as the Board may call for.	

Processing by State and its instrumentalities Rule 5 + Schedule II of Final Rules (Under S. 7(b) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
~~**(1)** The State and any of its instrumentalities may process the personal data of a Data Principal under clause (b) of section 7 of the Act to provide or to issue to her any subsidy, benefit, service, certificate, licence or permit that is provided or issued under law or policy or using public funds.~~	**(1)** Processing the personal data of a Data Principal under this rule shall be done following the standards specified in Second Schedule. **(2)** In this rule and the Second Schedule, the reference to any subsidy, benefit, service, certificate, licence or permit that is provided or issued—	**1. Deletion of redundant language:** The substantive content of the earlier sub-clause (1) was covered under Section 7(b) of the Act, and is therefore removed from this Rule. **2. Enhanced data quality obligations for the State: for the State** The Final Rules add explicit obligations on the State to ensure

(2) Processing under this rule shall be done following the standards specified in Second Schedule. **(3)** In this rule and Second Schedule, the reference to any subsidy, benefit, service, certificate, licence or permit that is provided or issued— (a) under law shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit in exercise of any power of or the performance of any function by the State or any of its instrumentalities under any law for the time being in force; (b) under policy shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit under any policy or instruction issued by the Central Government or a State Government in exercise of its executive power; and (c) using public funds shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit by incurring expenditure on the same from, or with accrual of receipts to,— (i) in case of the Central Government or a State Government, the Consolidated Fund of India or the Consolidated Fund of the State	(a) under law shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit in exercise of any power of or the performance of any function by the State or any of its instrumentalities under any law for the time being in force; (b) under policy shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit under any policy or instruction issued by the Central Government or a State Government in exercise of its executive power; and (c) using public funds shall be construed as a reference to provision or issuance of such subsidy, benefit, service, certificate, licence or permit by incurring expenditure on the same from, or with accrual of receipts to, — (i) in case of the Central Government or a State Government, the Consolidated Fund of India or the Consolidated Fund of the State or the public account of India or the public account of the State; or (ii) in case of any local or other authority within the territory of India or under the control of the Government of India or of any State, the fund or funds of such authority.	completeness, accuracy, and consistency of processing personal data when providing subsidies, benefits, certificates, licences, or permits. The addition elevates the data-quality obligations of the State, ensuring that all public-benefit decisions rely on reliable, error-free personal data and reducing wrongful denials or administrative mistakes.

or the public account of India or the public account of the State; or (ii) in case of any local or other authority within the territory of India or under the control of the Government of India or of any State, the fund or funds of such authority.		

Reasonable Security Safeguards Rule 6 of Final Rules (Under S. 8(5) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum,— (a) appropriate data security measures, ~~including~~ securing of such personal data through ~~its~~ encryption, obfuscation ~~or~~ masking or the use of virtual tokens mapped to that personal data; (b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor; (c) visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and	**(1)** A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum, — (a) appropriate data security measures, such as securing of personal data through encryption, obfuscation, masking or the use of virtual tokens mapped to that personal data; (b) appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor, wherever applicable; (c) visibility on the accessing of such personal data, through appropriate logs, monitoring and review, for enabling detection of unauthorised access, its investigation and remediation to prevent recurrence;	**Inclusion of suggestive reasonable security practices:** The Final Rules replace 'including' with 'such as' for the various examples of reasonable security safeguards listed under the Final Rules. This change makes the listed practices merely indicative based on their relevance to the data management practices of the Data Fiduciary. However, the broader principle underlying each measure would still need to be implemented (i.e. appropriate data security measures, appropriate measures to control access to the computer resources, visibility on the accessing of personal data etc.)

remediation to prevent recurrence; (d) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, ~~including~~ by way of data backups; (e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise; (f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards; and (g) appropriate technical and organisational measures to ensure effective observance of security safeguards. **(2)** In this rule, the expression "computer resource" shall have the same meaning as is assigned to it in Information Technology Act, 2000 (21 of 2000).	(d) reasonable measures for continued processing in the event of confidentiality, integrity or availability of such personal data being compromised as a result of destruction or loss of access to personal data or otherwise, such as by way of data-backups; (e) for enabling the detection of unauthorised access, its investigation, remediation to prevent recurrence and continued processing in the event of such a compromise, retain such logs and personal data for a period of one year, unless compliance with any law for the time being in force requires otherwise; (f) appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor, wherever applicable, for taking reasonable security safeguards; and (g) appropriate technical and organisational measures to ensure effective observance of security safeguards. **(2)** In this rule, the expression "computer resource" shall have the same meaning as is assigned to it in Information Technology Act, 2000 (21 of 2000).	

Intimation of Personal Data Breach Rule 7 of Final Rules (Under S. 8(6) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered by her with the Data Fiduciary,— (a) a description of the breach, including its nature, extent and the timing ~~and location~~ of its occurrence; (b) the consequences relevant to her, that are likely to arise from the breach; (c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk; (d) the safety measures that she may take to protect her interests; and (e) business contact information of a person who is able to respond on behalf of the Data Fiduciary, to queries, if any, of the Data Principal. **(2)** On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board,— (a) without delay, a description	**(1)** On becoming aware of any personal data breach, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay, through her user account or any mode of communication registered by her with the Data Fiduciary, — (a) a description of the breach, including its nature, extent and the timing of its occurrence; (b) the consequences relevant to her, that are likely to arise from the breach; (c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk; (d) the safety measures that she may take to protect her interests; and (e) business contact information of a person who is able to respond on behalf of the Data Fiduciary, to queries, if any, of the Data Principal. **(2)** On becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board, — (a) without delay, a description of the breach, including its nature,	**1. Location reporting limited to Board:** The Final Rules remove the requirement of Data Fiduciaries to intimate to its Data Principals the location of the breach, however, it still needs to be intimated to the DPB. The change limits Data Principal's awareness about breach origins. **2. Retention of 72-hour reporting timeline:** The Final Rules maintain the requirement for Data Fiduciaries to provide detailed breach reports to the DPB within 72 hours of becoming aware of the breach, with DPB's discretion to grant extensions upon written request.

of the breach, including its nature, extent, timing and location of occurrence and the likely impact; (b) within seventy-two hours of becoming aware of the ~~same~~, or within such longer period as the Board may allow on a request made in writing in this behalf,— (i) updated and detailed information in respect of such description; (ii) the broad facts related to the events, circumstances and reasons leading to the breach; (iii) measures implemented or proposed, if any, to mitigate risk; (iv) any findings regarding the person who caused the breach; (v) remedial measures taken to prevent recurrence of such breach; and (vi) a report regarding the intimations given to affected Data Principals. **(3)** In this rule, "user account" means the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such Data Principal is able to access the services of such Data Fiduciary.	extent, timing and location of occurrence and the likely impact; (b) within seventy-two hours of becoming aware of the breach, or within such longer period as the Board may allow on a request made in writing in this behalf, — (i) updated and detailed information in respect of such description; (ii) the broad facts related to the events, circumstances and reasons leading to the breach; (iii) measures implemented or proposed, if any, to mitigate risk; (iv) any findings regarding the person who caused the breach; (v) remedial measures taken to prevent recurrence of such breach; and (vi) a report regarding the intimations given to affected Data Principals.	

Time period for specified purpose to be deemed as no longer being served Rule 8 + Schedule III of Final Rules (Under S. 8(8) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) A Data Fiduciary, who is of such class and is processing personal data for such corresponding purposes as are specified in Third Schedule, shall erase such personal data, unless its retention is necessary for compliance with any law for the time being in force, if, for the corresponding time period specified in the ~~said~~ Schedule, the Data Principal neither approaches such Data Fiduciary for the performance of the specified purpose nor exercises her rights in relation to such processing. **(2)** At least forty-eight hours before completion of the time period for erasure of personal data under this rule, the Data Fiduciary shall inform the Data Principal that such personal data shall be erased upon completion of such period, unless she logs into her user account or otherwise initiates contact with the Data Fiduciary for the performance of the specified purpose or exercises her rights in relation to the processing of such personal data. ~~**(3)** In this rule, "user account" means the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile~~	**(1)** A Data Fiduciary, who is of such class and is processing personal data for such corresponding purposes as are specified in Third Schedule, shall erase such personal data, unless its retention is necessary for compliance with any law for the time being in force, or, for the corresponding time period specified in the Third Schedule, if the Data Principal neither approaches such Data Fiduciary for the performance of the specified purpose nor exercises her rights in relation to such processing. **(2)** At least forty-eight hours before completion of the time period for erasure of personal data under this rule, the Data Fiduciary shall inform the Data Principal that such personal data shall be erased upon completion of such period, unless she logs into her user account or otherwise initiates contact with the Data Fiduciary for the performance of the specified purpose or exercises her rights in relation to the processing of such personal data. **(3)** Without prejudice to sub-rules (1) and (2), a Data Fiduciary shall retain, in respect of **any processing of personal data undertaken by it or on its behalf by a Data Processor, such personal data, associated**	**1. Universal 1 year minimum retention:** The Final Rules introduce new Sub-rule 8(3) mandating that all Data Fiduciaries must retain personal data, associated traffic data, and processing logs for a minimum of 1 year from the date of processing. This retention serves purposes specified in Schedule VII including state sovereignty and security interests, performance of functions under law, disclosure requirements for legal obligations, and assessment for Significant Data Fiduciary classification. **2. Data Processor obligations:** The 1 year retention requirement also extends to Data Processors. Data Fiduciaries must ensure their processors retain data and logs for the minimum 1 year period. **3. Longer retention timeline for specified entities:** The 1 year baseline retention operates alongside the 3 year timeline for specified entities under sub-rule 8(1) read with Schedule III. The following entities must retain data for 3 years from the date the Data Principal last approached the Data Fiduciary or exercised rights, whichever is latest: • E-commerce entities with 2 crore+ users • Online gaming intermediaries with 50 lakh+ users

~~number and other similar presences by means of which she is able to access the services of such Data Fiduciary.~~	**traffic data and other logs of the processing for a minimum period of one year from the date of such processing, for the purposes as specified in the Seventh Schedule**, after which the Data Fiduciary shall cause such personal data and logs to be erased, unless further retention is required for compliance with any other law for the time being in force or notified by the Government.	• Social media intermediaries with 2 crore+ users

Contact information of person to answer questions about processing Rule 9 of Final Rules (Under S. 8(9) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
Every Data Fiduciary shall prominently publish on its website or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business contact information of the Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data.	Every Data Fiduciary shall prominently publish on its website or app, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business contact information of the Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data.	No change

Verifiable consent for processing of personal data of child Rule 10 of Final Rules (Under S. 9 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent	**(1)** A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of	**1. Separation of child and disability provisions:** The Draft Rule 10 covered both children and persons with disability in a

of the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to— (a) reliable details of identity and age available with the Data Fiduciary; or (b) voluntarily provided details of identity and age or a virtual token mapped to ~~the same~~, which is issued by an ~~entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider~~. ~~**(2)** A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such guardian is appointed by a court of law, a designated authority or a local level committee, under the law applicable to guardianship.~~ **(3)** In this rule, the expression— (a) "adult" shall mean an individual who has completed	the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to— (a) reliable details of identity and age of the individual available with the Data Fiduciary; or (b) details of identity and age, voluntarily provided — (i) by the individual; or (ii) through a virtual token mapped to such details, which is issued by an authorised entity. **(2)** In this rule, the expression— (a) "adult" shall mean an individual who has completed the age of eighteen years; (b) "authorised entity" shall mean — (i) an entity entrusted by law or by the Central Government or by the State Government with the issuance of details of the identity and age or a virtual token mapped to such details; or (ii) a person appointed or permitted by the entity specified under clause (i), for such issuance, and also includes details of identity and age or token made available and verified by a Digital Locker Service Provider; (c) "Digital Locker service provider" shall mean such intermediary, including a body	combined provision. The Final Rules separate these into distinct rules. **Distinct consent verification pathways:** This separation reflects operational differences in consent verification. For children, the critical requirement is confirming whether the parent is an identifiable adult. For persons with disability, Rule 11 establishes a more stringent standard requiring verification that the guardian was legally appointed by a court, designated authority, or local level committee under specialized guardianship laws. 2**. Introduction of "authorised entity" definition:** The Final Rules introduce "authorized entity" in Rule 10(2)(b) to define entities empowered to issue credentials for parental age verification. An authorized entity may issue (i) details of identity and age of individuals, or (ii) virtual tokens mapped to such identity and age details. This enables Data Fiduciaries to verify parental consent by relying on credentials from government-designated identity authorities or their appointees. **Primary and delegated issuers:** The authorized entity definition establishes a two-tier structure. Primary issuers comprise entities formally empowered by law or designated by Central or State Government to issue identity/age credentials or virtual tokens. Delegated issuers include persons appointed or permitted by these primary entities to carry out credential issuance on their

the age of eighteen years; (b) "Digital Locker service provider" shall mean such intermediary, including a body corporate or an agency of the appropriate Government, as may be notified by the Central Government, in accordance with the rules made in this regard under the Information Technology Act, 2000 (21 of 2000); ~~(c) "designated authority" shall mean an authority designated under section 15 of the Rights of Persons with Disabilities Act, 2016 (49 of 2016) to support persons with disabilities in exercise of their legal capacity;~~ ~~(d) "law applicable to guardianship" shall mean,—~~ ~~(i) in relation to an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who despite being provided adequate and appropriate support is unable to take legally binding decisions, the provisions of law contained in Rights of Persons with Disabilities Act, 2016 (49 of 2016) and the rules made thereunder; and~~ ~~(ii) in relation to a person who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of such conditions and includes a person suffering from severe~~	corporate or an agency of the appropriate Government, as may be notified by the Central Government, in accordance with the rules made in this regard under the Information Technology Act, 2000 (21 of 2000);	behalf. This structure may enable primary entities to scale verification services through authorized intermediaries while maintaining regulatory oversight over the credential issuance chain.

~~multiple disability, the provisions of law of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999) and the rules made thereunder;~~ ~~(e) "local level committee" shall mean a local level committee constituted under section 13 of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999);~~ ~~(f) "person with disability" shall mean and include—~~ ~~(i) an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions; and~~ ~~(ii) an individual who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and includes an individual suffering from severe multiple disability.~~		

Verifiable consent for processing of personal data of person with disability who has lawful guardian Rule 11 of Final Rules (Under S. 9(1) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) ~~A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child and shall observe due diligence, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to —~~ ~~(a) reliable details of identity and age available with the Data Fiduciary; or~~ ~~(b) voluntarily provided details of identity and age or a virtual token mapped to the same, which is issued by an entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider.~~ **(2)** A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such guardian is appointed by a court of law, a designated	**(1)** A Data Fiduciary, while obtaining verifiable consent from an individual identifying herself as the lawful guardian of a person with disability, shall observe due diligence to verify that such guardian is appointed by a court of law, or by a designated authority or by a local level committee, under the law applicable to guardianship. **(2)** In this rule, the expression— (a) "designated authority" shall mean an authority designated under section 15 of the Rights of Persons with Disabilities Act, 2016 (49 of 2016) to support persons with disabilities in exercise of their legal capacity; (b) "law applicable to guardianship" shall mean, — (i) in relation to an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who despite being provided adequate and appropriate support is unable to take legally binding decisions, the provisions of law contained in Rights of Persons with Disabilities Act, 2016 (49 of 2016) and the rules made thereunder; and (ii) in relation to a person who is suffering from any of the conditions relating to autism,	**1. The definition now explicitly adopts the "supported decision-making first" principle.** By adding this phrase, the final rules make it clear that guardianship is not presumed merely because a person has a disability. A Data Fiduciary can rely on guardian-consent only when: • The individual is a person with disability, • They have been offered adequate and appropriate support to make their own decision, and • Despite this support, they are unable to take a legally binding decision. **2. "Means and Includes" interpretive scope:** The Final Rules retain "person with disability shall mean and include" as an inclusive definition, potentially allowing additional disability categories beyond those enumerated. However, any such expansion must be construed narrowly through purposive interpretation - the guardian consent should apply only to persons with disabilities who, despite being provided adequate and appropriate support, are unable to take legally binding decisions.

authority or a local level committee, under the law applicable to guardianship. **(3)** In this rule, the expression— ~~(a) "adult" shall mean an individual who has completed the age of eighteen years;~~ ~~(b) "Digital Locker service provider" shall mean such intermediary, including a body corporate or an agency of the appropriate Government, as may be notified by the Central Government, in accordance with the rules made in this regard under the Information Technology Act, 2000 (21 of 2000);~~ (c) "designated authority" shall mean an authority designated under section 15 of the Rights of Persons with Disabilities Act, 2016 (49 of 2016) to support persons with disabilities in exercise of their legal capacity; (d) "law applicable to guardianship" shall mean,— (i) in relation to an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who despite being provided adequate and appropriate support is unable to take legally binding decisions, the provisions of law contained in Rights of Persons with Disabilities Act, 2016 (49 of 2016) and the rules made thereunder; and	cerebral palsy, mental retardation or a combination of such conditions and includes a person suffering from severe multiple disability, the provisions of law of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999) and the rules made thereunder; (c) "local level committee" shall mean a local level committee constituted under section 13 of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999); (d) "person with disability" shall mean and include— (i) an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions; and (ii) an individual who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and includes an individual suffering from severe multiple disability and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions.	

(ii) in relation to a person who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of such conditions and includes a person suffering from severe multiple disability, the provisions of law of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999) and the rules made thereunder; (e) "local level committee" shall mean a local level committee constituted under section 13 of the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 (44 of 1999); (f) "person with disability" shall mean and include— (i) an individual who has long term physical, mental, intellectual or sensory impairment which, in interaction with barriers, hinders her full and effective participation in society equally with others and who, despite being provided adequate and appropriate support, is unable to take legally binding decisions; and (ii) an individual who is suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and includes an individual suffering from severe multiple disability.		

Exemptions from certain obligations applicable to processing of personal data of child Rule 12 + Schedule IV of Final Rules (Under S. 9(4) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child by such class of Data Fiduciaries as are specified in Part A of Fourth Schedule, subject to such conditions as are specified in the said Part. **(2)** The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child for such purposes as are specified in Part B of Fourth Schedule, subject to such conditions as are specified in the said Part.	**(1)** The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child by such class of Data Fiduciaries as are specified in Part A of Fourth Schedule, subject to such conditions as are specified in the said Part. **(2)** The provisions of sub-sections (1) and (3) of section 9 of the Act shall not be applicable to processing of personal data of a child for such purposes as are specified in Part B of Fourth Schedule, subject to such conditions as are specified in the said Part.	**Modified exemptions for child data processing under revised Schedule IV:** **1. New real-time location tracking exemption:** Under the DPDP Act, Data Fiduciaries are prohibited from tracking or behaviourally monitoring children or conducting targeted advertising directed at them. The Final Rules introduce a new exemption to the DPDP Act's prohibition - tracking to determine a child's real-time location when necessary for her safety, security, or protection. **2. Expanded harmful content prevention:** The Draft Rules permitted tracking only to restrict a child's access to "information" likely to be detrimental to her well-being. The Final Rules expand this to "information, service, or advertisement" that could adversely impact a child's well-being. This allows broader protective monitoring, such as filtering harmful services or blocking age-inappropriate advertisements.

Additional obligations of Significant Data Fiduciary Rule 13 of Final Rules (Under S. 10 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) A Significant Data Fiduciary shall, once in every period of twelve months from the date on which it is notified as such or is included in the class of Data	**(1)** A Significant Data Fiduciary shall, once in every period of twelve months from the date on which it is notified as such or is included in the class of Data	**1. Scope expanded from only algorithms → technical measures.** The Final Rule clarifies that algorithmic software is only one part of a wider category of

Fiduciaries notified as such, undertake a Data Protection Impact Assessment and an audit to ensure effective observance of the provisions of this Act and the rules made thereunder. **(2)** A Significant Data Fiduciary shall cause the person carrying out the Data Protection Impact Assessment and audit to furnish to the Board a report containing significant observations in the Data Protection Impact Assessment and audit. **(3)** A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software ~~deployed~~ by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals. **(4)** A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government on the basis of the recommendations of a committee constituted by it is processed subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.	Fiduciaries notified as such, undertake a Data Protection Impact Assessment and an audit to ensure effective observance of the provisions of this Act and the rules made thereunder. **(2)** A Significant Data Fiduciary shall cause the person carrying out the Data Protection Impact Assessment and audit to furnish to the Board a report containing significant observations in the Data Protection Impact Assessment and audit. **(3)** A Significant Data Fiduciary shall observe due diligence to verify that technical measures including algorithmic software adopted by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals. (4) A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government, on the basis of the recommendations of a committee constituted by it, is processed subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India. **(5)** In this rule, "committee" means a committee constituted by the Central Government for the purpose of this rule, which shall include officials from the Ministry of Electronics and Technology and may include officials from other Ministries or Department of the Central Government.	technical measures, widening the scope of due diligence and risk assessments conducted by SDFs. **2. Responsibility applies to systems "adopted" by the SDF, not only "deployed":** SDFs are accountable for third-party tech, not just their in-house tools. This means: • vendor due diligence becomes mandatory, • third-party risk management must be strengthened, • SDF must prove it evaluated risks before adopting any external tech. **3. The "committee" is now formally defined**: The Final Rules define the composition of the committee constituted by the Central Government that will recommend data localization restrictions, giving these decisions legal clarity, administrative legitimacy, and reduced judicial vulnerability.

Rights of Data Principals Rule 14 of Final Rules (Under Ss. 11-14 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) For enabling Data Principals to exercise their rights under the Act, the Data Fiduciary and, where applicable, the Consent Manager, shall publish on its website or app, or both, as the case may be, — (a) the details of the means using which a Data Principal may make a request for the exercise of such rights; and (b) the particulars, if any, such as the username or other identifier of such a Data Principal, which may be required to identify her under its terms of service. **(2)** To exercise the rights of the Data Principal under the Act ~~to access information about personal data and its erasure,~~ she may make a request to the Data Fiduciary to whom she has previously given consent for processing of her personal data, using the means and furnishing the particulars published by such Data Fiduciary for the exercise of such rights. **(3)** Every Data Fiduciary and Consent Manager shall publish on its website or app, or both, as the case may be, the period under its grievance redressal system for responding to the grievances of Data Principals and shall, for ensuring the	**(1)** For enabling Data Principals to exercise their rights under the Act, the Data Fiduciary and, where applicable, the Consent Manager, shall prominently publish on its website or app, or both, as the case may be, — (a) the details of the means using which a Data Principal may make a request for the exercise of such rights; and (b) the particulars, if any, such as the username or other identifier of such a Data Principal, which may be required to identify her under its terms of service. **(2)** To exercise the rights of the Data Principal under the Act, she may make a request to the Data Fiduciary to whom she has previously given consent for processing of her personal data, using the means and furnishing the particulars required by such Data Fiduciary for the exercise of such rights. **(3)** Every Data Fiduciary and Consent Manager shall prominently publish on its website or app, or both, as the case may be, within a reasonable period not exceeding ninety days under its grievance redressal system for responding to the grievances of Data Principals and shall, for ensuring the effectiveness of the system in responding within such period,	**1. Grievance resolution period clarified:** Data Fiduciaries must publicly display their grievance-handling timeline, on websites, apps, or notices. This prevents arbitrary, undisclosed or excessively long internal timelines. Clearly defined grievance periods encourage trust and align India's regime more closely with global best practice grievance-handling norms. **2. Addition of email address and phone numbers as identifiers:** The rule now lists email address and phone number as examples of identifiers used to verify the Data Principal's identity. This reduces ambiguity and ensures smoother, digital-friendly rights-request workflows.

effectiveness of the system in responding within such period, implement appropriate technical and organisational measures. **(4)** To exercise the rights of the Data Principal under the Act ~~to nominate~~, she may, in accordance with the terms of service of the Data Fiduciary and such law as may be applicable, nominate one or more individuals, using the means and furnishing the particulars ~~published~~ by such Data Fiduciary for the exercise of such right. **(5)** In this rule, the expression "identifier" shall mean any sequence of characters issued by the Data Fiduciary to identify the Data Principal and includes a customer identification file number, customer acquisition form number, application reference number, enrolment ID or licence number that enables such identification.	implement appropriate technical and organisational measures. **(4)** To exercise the rights of the Data Principal under the Act, she may, in accordance with the terms of service of the Data Fiduciary and such law as may be applicable, nominate one or more individuals, using the means and furnishing the particulars required by such Data Fiduciary for the exercise of such right. **(5)** In this rule, the expression "identifier" shall mean any sequence of characters issued by the Data Fiduciary to identify the Data Principal and includes a customer identification file number, customer acquisition form number, application reference number, enrolment ID, email address, mobile number or licence number that enables such identification	

Processing of personal data outside India Rule 15 of Final Rules (Under S. 16 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
Transfer to any country or territory outside India of ~~personal data processed by a Data Fiduciary — (a) within the territory of India; or (b) outside the territory of India in connection with any activity related to offering of goods or services to Data Principals~~	Clause title changed to - **Transfer of personal data outside the territory of India.** Any personal data processed by a Data Fiduciary under the Act may be transferred outside the territory of India subject to the restriction that the Data Fiduciary shall meet such requirements as	**1. India shifts to a broad "permit-by-default" model for cross-border data flows.** The revised clause now provides that "any personal data processed by a Data Fiduciary under the Act" may be transferred outside India, regardless of the physical location where initial processing occurred.

~~within the territory of India,~~ is subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, 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 Central Government may, by general or special order, 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 new formulation makes it clearer that cross-border processing is the norm, and restrictions are the exception. **2. Government restriction mechanism**: The Central Government retains discretionary power to publish a blacklist of prohibited destination countries or territories through official gazette notifications. This executive notification mechanism enables swift policy responses to evolving geopolitical circumstances without requiring legislative amendments.

Exemption from Act for research, archiving or statistical purposes Rule 16 + Schedule II of Final Rules (Under S. 17(2)(b) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with the standards specified in Second Schedule.	The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with the standards specified in Second Schedule.	No change

Appointment of Chairperson and other Members Rule 17 of Final Rules (Under S. 19 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) The Central Government shall constitute a Search-cum-Selection Committee, with the Cabinet Secretary as the chairperson and the Secretaries to the Government of India in charge of the Department of Legal Affairs and the Ministry of Electronics and Information	**(1)** The Central Government shall constitute a Search-cum-Selection Committee, with the Cabinet Secretary as the chairperson and the Secretaries to the Government of India in charge of the Department of Legal Affairs and the Ministry of Electronics and Information Technology and	**1. Both committees now enjoy immunity from procedural challenges.** Earlier, only the proceedings of selection of the Chairperson was protected. Now, the Members' selection committee's procedure is also protected. The change ensures that

Technology and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as Chairperson. **(2)** The Central Government shall constitute a Search-cum-Selection Committee, with the Secretary to the Government of India in the Ministry of Electronics and Information Technology as the chairperson and the Secretary to the Government of India in charge of the Department of Legal Affairs, and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as a Member other than the Chairperson. **(3)** The Central Government shall, after considering the suitability of individuals recommended by the Search-cum-Selection Committee, appoint the Chairperson or other Member, as the case may be. **(4)** No act or proceeding of the Search-cum-Selection Committee specified in sub-rules (1) of this rule shall be called in question on the ground merely of the existence of any vacancy or absences in such committee or defect in its constitution.	two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as Chairperson. **(2)** The Central Government shall constitute a Search-cum-Selection Committee, with the Secretary to the Government of India in the Ministry of Electronics and Information Technology as the chairperson and the Secretary to the Government of India in charge of the Department of Legal Affairs, and two experts of repute having special knowledge or practical experience in a field which in the opinion of the Central Government may be useful to the Board as members, to recommend individuals for appointment as a Member other than the Chairperson. **(3)** The Central Government shall, after considering the suitability of individuals recommended by the Search-cum-Selection Committee, appoint the Chairperson or other Member, as the case may be. **(4)** No act or proceeding of the Search-cum-Selection Committee specified in sub-rules (1) and (2) of this rule shall be called in question on the ground merely of the existence of any vacancy or absences in such committee or defect in its constitution	appointments of both the Chairperson and Members of the DPB are protected from being challenged on technical grounds, thereby strengthening administrative continuity and preventing delays.

Salary, allowances and other terms and conditions of service of Chairperson and other Members Rule 18 + Schedule V of Final Rules (Under S. 20 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
The Chairperson and every other Member shall receive such salary and allowances and shall have such other terms and conditions of service as are specified in Fifth Schedule.	The Chairperson and every other Member shall receive such salary and allowances and shall have such other terms and conditions of service as are specified in Fifth Schedule.	No change

Procedure for meetings of Board and authentication of its orders, directions and instruments Rule 19 of Final Rules (Under S. 23 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) The Chairperson shall fix the date, time and place of meetings of the Board, approve the items of agenda therefor, and cause notice specifying the same to be issued under her signature or that of such other individual as the Chairperson may authorise by general or special order in writing. **(2)** Meetings of the Board shall be chaired by the Chairperson and, in her absence, by such other Member as the Members present at the meeting may choose from amongst themselves. **(3)** One-third of the membership of the Board shall be the quorum for its meetings. **(4)** All questions which come up before any meeting of the Board shall be decided by a majority of the votes of Members present and voting, and, in the event of an equality of votes, the Chairperson, or in her absence, the person chairing, shall have a second or casting vote.	**(1)** The Chairperson shall fix the date, time and place of meetings of the Board, approve the items of agenda therefore, and cause notice specifying the same to be issued under her signature or that of such other individual as the Chairperson may authorise by general or special order in writing. **(2)** Meetings of the Board shall be chaired by the Chairperson and, in her absence, by such other Member as the Members present at the meeting may choose from amongst themselves. **(3)** One-third of the membership of the Board shall be the quorum for its meetings. **(4)** All questions which come up before any meeting of the Board shall be decided by a majority of the votes of Members present and voting, and, in the event of an equality of votes, the Chairperson, or in her absence, the person chairing, shall have a second or casting vote.	No change

(5) If a Member has an interest in any item of business to be transacted at a meeting of the Board, she shall not participate in or vote on the same and, in such a case, the decision on such item shall be taken by a majority of the votes of other Members present and voting. **(6)** In case an emergent situation warrants immediate action by the Board and it is not feasible to call a meeting of the Board, the Chairperson may, while recording the reasons in writing, take such action as may be necessary, which shall be communicated within seven days to all Members and laid before the Board for ratification at its next meeting. **(7)** If the Chairperson so directs, an item of business or issue which requires decision of the Board may be referred to Members by circulation and such item may be decided with the approval of majority of the Members. **(8)** The Chairperson or any Member of the Board, or any individual authorised by it by a general or special order in writing, may, under her signature, authenticate its order, direction or instrument. **(9)** The inquiry by the Board shall be completed within a period of six months from the date of receipt of the intimation, complaint, reference or direction under section 27 of the Act, unless such period is extended by it, for reasons to be recorded in writing, for a further period not exceeding three months at a time.	**(5)** If a Member has an interest in any item of business to be transacted at a meeting of the Board, she shall not participate in or vote on the same and, in such a case, the decision on such item shall be taken by a majority of the votes of other Members present and voting. **(6)** In case an emergent situation warrants immediate action by the Board and it is not feasible to call a meeting of the Board, the Chairperson may, while recording the reasons in writing, take such action as may be necessary, which shall be communicated within seven days to all Members and laid before the Board for ratification at its next meeting. **(7)** If the Chairperson so directs, an item of business or issue which requires decision of the Board may be referred to Members by circulation and such item may be decided with the approval of majority of the Members. **(8)** The Chairperson or any Member of the Board, or any individual authorised by it,by a general or special order in writing, may, under her signature, authenticate its order, direction or instrument. **(9)** The inquiry by the Board shall be completed within a period of six months from the date of receipt of the intimation, complaint, reference or direction under section 27 of the Act, unless such period is extended by it, for reasons to be recorded in writing, for a further period not exceeding three months at a time	

Functioning of Board as digital office Rule 20 of Final Rules (Under S. 28(1) DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
The Board shall function as a digital office which, without prejudice to its power to summon and enforce the attendance of any person and examine her on oath, may adopt techno-legal measures to conduct proceedings in a manner that does not require physical presence of any individual.	The Board shall function as a digital office, without prejudice to its power to summon and enforce the attendance of any person and examine her on oath, may adopt techno-legal measures to conduct proceedings in a manner that does not require physical presence of any individual	No change

Terms and conditions of appointment and service of officers and employees of Board Rule 21 + Schedule VI of Final Rules (Under S. 24 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) The Board may, with previous approval of the Central Government ~~and in such manner as the Central Government may by general or special order specify,~~ appoint such officers and employees as it may deem necessary for the efficient discharge of its functions under the provisions of the Act. **(2)** The terms and conditions of service of officers and employees of the Board shall be such as are specified in Sixth Schedule.	**(1)** The Board may, with previous approval of the Central Government, appoint such officers and employees as it may deem necessary for the efficient discharge of its functions under the provisions of the Act. **(2)** The terms and conditions of service of officers and employees of the Board shall be such as are specified in Sixth Schedule.	**No substantive change:** Removal of requirement that Central Govt. must "specify manner" of appointment.

Appeal to Appellate Tribunal Rule 22 of Final Rules (Under S. 29 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) ~~An appeal, including any related documents, by a~~ person aggrieved by an order or direction of the Board, shall be filed in digital form, ~~following such procedure as may be specified by the Appellate Tribunal on its website.~~ **(2)** An appeal filed with the Appellate Tribunal shall be accompanied by fee of like amount as is applicable in respect of an appeal filed under the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), unless reduced or waived by the Chairperson of the Appellate Tribunal at her discretion, and the same shall be payable digitally using the Unified Payments Interface or such other payment system authorised by the Reserve Bank of India ~~as the Appellate Tribunal may specify on its website.~~ **(3)** The Appellate Tribunal— (a) shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the provisions of the Act, may regulate its own procedure; and (b) shall function as a digital office which, without prejudice	**(1)** Any person aggrieved by an order or direction of the Board, may prefer an appeal before the Appellate Tribunal, it shall be filed in digital form as the Appellate Tribunal may decide. **(2)** An appeal filed with the Appellate Tribunal shall be accompanied by fee of like amount as is applicable in respect of an appeal filed under the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), unless reduced or waived by the Chairperson of the Appellate Tribunal at her discretion, and the same shall be payable digitally using the Unified Payments Interface or such other payment system authorised by the Reserve Bank of India. **(3)** The Appellate Tribunal— (a) shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the provisions of the Act, may regulate its own procedure; and (b) shall function as a digital office which, without prejudice to its power to summon and enforce the attendance of any person and examine her on oath, may adopt techno-legal measures to conduct	**No substantive change:** Wording simplified; procedural substance identical.

to its power to summon and enforce the attendance of any person and examine her on oath, may adopt technolegal measures to conduct proceedings in a manner that does not require physical presence of any individual.	proceedings in a manner that does not require physical presence of any individual.	

Calling for information from Data Fiduciary or intermediary Rule 23 + Schedule VII of Final Rules (Under S. 36 DPDP Act)		
Draft Rules	**Final Rules**	**Implication of Changes**
(1) The Central Government may, for such purposes of the Act as are specified in Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, specify the time period within which the same shall be furnished and, where disclosure in this regard is likely to prejudicially affect the sovereignty and integrity of India or security of the State, require the Data Fiduciary or intermediary to not disclose the same except with the previous permission in writing of the authorised person. ~~**(2)** Provision of information called for under this rule shall be by way of fulfilment of obligation under section 36 of the Act.~~	**(1)** The Central Government may, for such purposes of the Act as are specified in Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, require any Data Fiduciary or intermediary to furnish such information as may be called for, within the specified period as may be given in such. **(2)** Where the disclosure of furnishing of information as referred to in sub-rule (1) is likely to prejudicially affect the sovereignty and integrity of India or security of the State, the Central Government may require the Data Fiduciary or intermediary to not disclose such furnishing to affected Data Principal or any other person except with the previous permission, in writing, of the authorised person. **(3)** For the purposes of this rule, the expression "intermediary" shall have the same meaning as assigned to it in the Information Technology Act, 2000 (21 of 2000)	**No substantive change:** Disclosure prejudicial to state has been split and added as a new sub clause.

References

1. Parliament of India. *The Digital Personal Data Protection Act, 2023* (No. 22 of 2023). Gazette of India, Extraordinary, Part II — Section 1, 11 August 2023.
Available at: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (meity.gov.in)

2. Ministry of Electronics and Information Technology (Draft). *Draft Digital Personal Data Protection Rules, 2025*. Government of India, 3 January 2025.
Available at: https://cdn.digitalindiacorporation.in/wp-content/uploads/2025/01/Draft-Digital-Personal-Data-Protection-Rules2025.pdf (cdn.digitalindiacorporation.in)

3. Ministry of Electronics and Information Technology. *Digital Personal Data Protection Rules, 2025*. Government of India Notification, 14 November 2025.
Available at: https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025 (meity.gov.in)

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