SUMMARY

DPDP (Draft) Rules, 2025

- Draft released for public consultation on: **3rd January 2025**
- The DPDP Rules, 2025 draft contains 22 Rules and 7 Schedules to complement the DPDP Act, of 2023.
- The DPDP Rules, 2025 hereinafter shall be referred to as "the Rules".

Rule 1: Short title and commencement.

i. The Rules will be referred to as – Digital Personal Data Protection Rules, 2025.

ii. The draft of the rules shall come into effect once published and notified via the Official Gazette, **except** the Rules 3-15, 21, and 22 shall come into effect/force separately as and when notified.

Observation – Why do the main and essential rules of this draft have a separate notification and effect/force date?

Rule 2: Definitions.

i. All expressions to have the same definition as assigned within the DPDP Act, 2023, unless otherwise specified or mentioned in these Rules.

Rule 3: Notice given by Data Fiduciary to Data Principal.

i. The notice to Data Principals must be clear, understandable, and independent of other information.

ii. It should provide a fair account of necessary details for informed consent, including, (a) An itemized description of personal data; and (b) The purpose of processing and related goods or services.

iii. Include a communication link to access the Fiduciary's website/app and details for, (a) Withdrawing consent; (b) Exercising rights under the Act; and (c) Filing complaints with the Board.

Rule 4: Registration and obligations of Consent Manager.

- The 1st (First) Schedule is to be read with the Rule 4.

- Bifurcated into two parts, - **Part A** [Detailing the Conditions of registration of Consent Manager] and **Part B** [Obligations of Consent Manager].

i. Consent Managers meeting conditions in **Part A** of the First Schedule can apply for registration.

ii. The Board may approve or reject applications after inquiry.

iii. Registered Consent Managers must fulfil obligations in **Part B** of the First Schedule.

iv. The Board can take corrective actions, suspend, or cancel registration for non-adherence, protecting Data Principals' interests.

v. Part A and Part B of Schedule 1 is as follows –

PART A: Conditions of registration of Consent Manager	**PART B: Obligations of Consent Manager**
1. The applicant must be a company incorporated in India. 2. The applicant must have adequate technical, operational, and financial capacity to fulfill its obligations. 3. The financial condition and general character of the applicant's management must be sound. 4. The applicant's net worth must be at least Rs.2 crore. 5. The applicant must have sufficient business prospects, capital structure, and earning potential. 6. Directors, key managerial personnel, and senior management must have a reputation for fairness and integrity. 7. The applicant's memorandum and articles of association must include	1. The Consent Manager must enable Data Principals to give, manage, review, and withdraw consent for processing their personal data, either directly or through another Data Fiduciary. 2. Personal data must not be readable by the Consent Manager during sharing or transfer. 3. The platform must maintain records of - (a) Consents given, denied, or withdrawn; (b) Notices related to consent requests; (c) Sharing of personal data with transferee Data Fiduciaries. 4. The Consent Manager must - (a) Provide Data Principals access to their records; (b) Share records in machine-readable form upon request; (c) Retain records for at least seven

provisions ensuring adherence to obligations and requiring Board approval for amendments. 8. Proposed operations must be in the interest of Data Principals. 9. Independent certification is required to ensure - (a) The interoperable platform complies with data protection standards; (b) Adequate technical and organizational measures are in place to meet standards and obligations.	years or longer if agreed upon. 5. The Consent Manager must maintain a website or app as the primary interface for its services. 6. The Consent Manager cannot subcontract or assign its obligations under the Act. 7. Reasonable measures must be taken to prevent personal data breaches. 8. The Consent Manager must act in a fiduciary capacity towards Data Principals. 9. The Consent Manager must avoid conflicts of interest with Data Fiduciaries. 10. Measures must prevent conflicts due to the interests of directors, key managerial personnel, or senior management. 11. Publish key information on the website or app, including details of promoters, directors, and significant shareholders. 12. Periodic audits must review technical controls, compliance, and adherence to obligations, with reports submitted to the Board. 13. The company's control cannot be transferred (e.g., through sale or merger) without prior Board approval.

Rule 5: Processing for provision or issue of subsidy, benefit, service, certificate, licence or permit by State and its instrumentalities.

- The 2nd (Second) Schedule is to be read with the Rule 5(2) and 15.

i. The State and its instrumentalities can process personal data to provide subsidies, benefits, or services under law, policy, or using public funds, following Second Schedule standards.

ii. Subsidies/benefits refer to those issued under law, policy, or funded by public finances like the Consolidated Fund or local authority funds.

Rule 6: Reasonable security safeguards.

i. Data Fiduciaries must protect personal data through, - (a) Encryption, masking, or virtual tokens; (b) Controlled access to computer resources; (c) Logs and monitoring to detect and address unauthorized access; (d) Backup and recovery measures in case of data loss; (e) Retaining logs for one year unless law requires otherwise; (f) Security clauses in contracts with Data Processors; (g) Technical and organizational measures for compliance.

ii. "Computer resource" has the meaning as per the IT Act, 2000.

Rule 7: Intimation of personal data breach.

i. **For the Affected Person** –

   a. Upon becoming aware of a breach, the Data Fiduciary must notify the affected Data Principal promptly with, (a) Details of the breach (nature, extent, timing, location); (b) Likely consequences; (c) Measures to mitigate risks; (d) Safety steps the Data Principal can take; and (e) Contact details of a person for queries.

ii. **To the DPBI** –

   a. Provide immediate **basic** details about the breach.

   b. And the detailed version of information within 72 hours, including causes, measures taken, and updates about notifications to Data Principals.

Rule 8: Time period for specified purpose to be deemed as no longer being served.

- The 3rd (Third) Schedule is to be read with the Rule 8(1).

i. Erase personal data if the Data Principal does not use the service or exercise rights for the specified time period unless retention is required by law.

ii. Notify the Data Principal 48 hours before data erasure, allowing them to log in or contact the Data Fiduciary to prevent erasure.

Rule 9: Contact information of person to answer questions about processing.

i. Publish the business contact details of the Data Protection Officer or an authorized person on the website/app and in responses to Data Principal queries about data processing.

Rule 10: Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian.

i. Obtain verifiable parental consent before processing a child's personal data.

ii. Ensure the person claiming to be the parent is an identifiable adult by verifying reliable identity and age details or tokens issued by authorized entities.

Rule 11: Exemptions from certain obligations applicable to processing of personal data of child.

- The 4th (Fourth) Schedule is to be read with the Rule 11.
- It is bifurcated in two parts, namely – **Part A** [Classes of Data Fiduciaries] and **Part B** [Purposes] – wherein in respect of whom provisions of section 9(1) and (3) of DPDP Act, 2023 shall not apply.

i. Exemptions from certain obligations under Section 9(1) and (3) apply:

   a. For specified classes of Data Fiduciaries (Part A of the Fourth Schedule).

   b. For specified purposes (Part B of the Fourth Schedule)

Rule 12: Additional obligations of Significant Data Fiduciary.

i. Conduct a Data Protection Impact Assessment and audit annually to ensure compliance with the Act and rules.

ii. Submit a report with significant observations from these assessments to the Board.

iii. Verify that algorithmic software does not pose risks to Data Principals' rights.

iv. Ensure specified personal data and traffic data remain within India based on government restrictions.

Rule 13: Rights of Data Principals.

i. Data Fiduciaries and Consent Managers must publish details on their website or app to enable Data Principals to:
   a. Submit requests for exercising their rights under the Act.
   b. Provide identifiers required for their identification as per terms of service.

ii. Data Principals can request access to or erasure of personal data from the Data Fiduciary they consented to, using the published means and identifiers.

iii. Data Fiduciaries and Consent Managers must publish grievance redressal timelines on their website or app and implement measures to meet these timelines.

iv. Data Principals can nominate individuals to act on their behalf, following the Data Fiduciary's terms of service and applicable law.

v. An "identifier" refers to a unique sequence of characters (e.g., customer ID, enrolment ID) issued by the Data Fiduciary.

Rule 14: Processing of personal data outside India.

i. Personal data processed by a Data Fiduciary within or outside India for offering goods or services in India can only be transferred abroad if the Data Fiduciary complies with requirements specified by the Central Government through general or special orders.

Rule 15: Exemption from Act for research, archiving or statistical purposes.

- The 2nd (Second) Schedule is to be read with the Rule 5(2) and 15.

i. The Act does not apply to personal data processing necessary for research, archiving, or statistical purposes, provided it meets the standards outlined in the Second Schedule.

Rule 16: Appointment of Chairperson and other Members.

i. A Search-cum-Selection Committee will be formed to recommend candidates for the Chairperson and Members:
   a. For the Chairperson, the Committee is led by the Cabinet Secretary and includes Secretaries from Legal Affairs and IT Ministries, along with two experts.
   b. For Members, the IT Secretary heads the Committee with Legal Affairs Secretary and two experts as members.

ii. The Central Government will appoint the Chairperson or Members based on the Committee's recommendations.

iii. The Committee's actions cannot be challenged on the basis of vacancies, absences, or defects in its constitution.

Rule 17: Salary, allowances and other terms and conditions of service of Chairperson and other Members.

- The 5th (Fifth) Schedule is to be read with the Rule 17.

i. Per the 5th Schedule the salary and allowances of the Chairperson and Members shall be -

Rule 18: Procedure for meetings of Board and authentication of its orders, directions and instruments.

i. Meetings of DPBI –

a. Meeting is arranged by the Chairperson. She decides the – date, time, and place and agenda for Board meetings, - issuing notice under her signature or an authorized individual's signature.

b. The Chairperson chairs meetings. In her absence, the Members present choose one among themselves to chair. At least one-third of the Board's members must be present for a meeting to proceed.

c. Majority Vote – required for decision making. In case of a tie, the Chairperson or Acting Chair will cast her vote.

d. Members with an interest in a matter cannot participate or vote on it. Such matters are decided by the other Members' majority vote.

e. Chairperson can act without calling a meeting (reasons to be recorded in writing) – only in urgent situations. Such action to be shared with Members within 7 days and ratified in next meeting.

f. With the Chairperson's direction, decisions may be taken by circulating the matter to Members and securing majority approval.

g. Orders, directions, or instruments are authenticated - under the signature of the Chairperson, a Member, or an authorized individual.

h. Board inquiries must be completed within six months, extendable by three months at a time with written reasons.

Rule 19: Functioning of Board as digital office.

i. The DPBI shall function as - (a) a digital office, i.e., there will be no physical court or premises; (b) will have the power to summon; (c) power to enforce the attendance of any person; (d) examine the individual on oath; (e) does not require the physical presence of any person; and (f) adoption of 'techno-legal' measures for conducting the proceedings.

Rule 20: Terms and conditions of appointment and service of officers and employees of Board.

- The 6th (Sixth) Schedule is to be read with the Rule 20(2).
- The schedule specifies the "terms and conditions of service of officers and employees of DPBI."

i. DPBI with - (a) prior approval of Central Government, and (b) Central Government's 'general' or 'special' manner – specify the appoint conditions of the board officers.

Rule 21: Appeal to Appellate Tribunal.

i. An appeal by any person aggrieved due to any order or direction of DPBI can be filed, - (a) The appeal is to be filed in '**digital form' only;** and (b) in the procedure specified by Appellate Tribunal on its website.

ii. The appeal shall bear a fee as suggested in the Telecom Regulatory Authority of India Act, 1997 (24 of 1997).

   a. The fee can be reduced or waived off at the discretion of the Appellate Tribunal.

   b. The fees shall be paid in digital form using payments systems approved by RBI or the UPI method, and such shall be mentioned on the Appellate Tribunal's website.

iii. Appellate Tribunal is - (a) NOT bound by CPC, 1908; (b) Follows the principle of Natural Justice; and (c) MAY regulate its own procedure.

   a. The Appellate Tribunal - (a) a digital office, i.e., there will be no physical court or premises; (b) will have the power to summon; (c) power to enforce the attendance of any person; (d) examine the individual on oath; (e) does not

require the physical presence of any person; and (f) adoption of 'techno-legal' measures for conducting the proceedings.

Rule 22: Calling for information from Data Fiduciary or intermediary.

- The 7th (Seventh) Schedule is to be read with the Rule 22(1).

i. The Central Government, through an authorized person specified in the Seventh Schedule, can require a Data Fiduciary or intermediary to provide information for purposes outlined in the Act. It can also set a deadline for furnishing the information and prohibit its disclosure (except with written permission) if such disclosure may harm India's sovereignty, integrity, or state security.

ii. Providing the requested information under this rule is considered an obligation under Section 36 of the Act.

Netlawgic Legal
602, Power Boulevard, Next to Passport Office, Koregaon Park Annex, Pune 411036
Tel +91 87110 06622 | office@netlawgic.com | www.netlawgic.com