Explanatory note to Digital Personal Data Protection Rules, 2025

The Digital Personal Data Protection Act, 2023 (Act) received the assent of the Hon'ble President on 11th August 2023. A draft of the Rules as envisaged under different sections of the Act have been made. The Rules provides for the necessary details and implementation framework of the Act.

During the drafting of Rules, certain principles used in the drafting of the Act, like using simple language, avoiding unnecessary cross referencing, providing contextual definition, and providing illustrations etc. have been followed meticulously. This explanatory note provides a brief overview of the contents of the Rules.

1. Short title and commencement: These rules, called the Digital Personal Data Protection Rules, 2025, come into force upon publication, except for rules 3 to 15, 21 and 22 which will be effective from a later date.

2. Definitions clause: The expression in the act shall have the same meaning as assigned in Act unless context otherwise requires.

3. Notice by Data Fiduciary to Data Principal: The notice provided by the Data Fiduciary to the Data Principal must be clear, standalone, and understandable, distinct from any other information shared by the Data Fiduciary. It must use simple, plain language to provide the Data Principal with a full and transparent account of the information necessary for giving informed consent for the processing of their personal data. Specifically, the notice should include, itemized list of the personal data being collected and clear description of the purpose for processing, along with an itemized explanation of the goods, services, or uses enabled by such processing.

Additionally, the notice must provide a communication link of the Data Fiduciary's website or app, and describe other methods (if applicable) for the Data Principal to withdraw consent easily as comparable to the process of giving consent, exercise their rights and make complaints with the Board.

4. Registration and obligations of a Consent Manager: Consent Manager must be a company incorporated in India with sound financial and operational capacity, having a minimum net worth of two crore rupees, a reputation for fairness and integrity in its management, and a certified interoperable platform enabling Data Principals to manage their consent.

The application for registration is to be made to the Board. Once registered, the Consent Manager must comply with specific obligations of ensuring that Data Principals can easily give, manage, review, and withdraw consent for data processing, maintaining records of consents and data sharing, and providing transparent access to such records. The Consent Manager is also required to implement strong security measures to protect personal data, avoid conflicts of interest, and ensure transparency by publishing key management details and ownership structures. Additionally, the Board may audit the Consent Manager's operations, suspend or cancel its registration if necessary, and issue corrective directions to safeguard the interests of Data Principals.

The Consent Manager must also maintain independence, with strict rules to prevent conflicts of interest involving its directors or senior management and Data Fiduciaries. They are prohibited from

Disclaimer: The purpose of this explanatory note is only to make it easier to understand the provisions of the Rules. However, this explanatory note is not intended to form part of the Rules and shall not be considered for legal interpretation of any provision of the Rules.

subcontracting or assigning responsibilities, and they must ensure long-term compliance by regularly reviewing their operations. Any transfer of control of the Consent Manager company, such as through sale or merger, requires prior approval from the Board. Through these provisions, the regulation ensures that Consent Managers uphold high standards of transparency, security, and fiduciary duty in managing personal data.

5. Processing for provision or issue of services by the State or its instrumentality: The State and its instrumentalities may process the personal data of Data Principals to provide or issue subsidies, benefits, services, certificates, licenses, or permits, as defined under law or policy or using public funds. Processing in these cases must adhere to the specific standards outlined in Schedule II, which ensures lawful, transparent, and secure handling of personal data for such purposes.

According to Schedule II, the processing must meet several key criteria, such as ensuring that personal data is processed lawfully, for the stated purposes, and limited to the data necessary for achieving those purposes. The data must be accurate and retained only as long as necessary, while appropriate security safeguards must be in place to prevent breaches. The Data Principal should be informed about the processing, including the means to access their rights, and the processing must be done in compliance with any applicable laws. The responsible parties must be accountable for adhering to these standards.

The aim is to ensure that personal data processing is transparent, secure, and in line with legal and policy standards, safeguarding the interests of the Data Principals.

6. Reasonable security safeguards: A Data Fiduciary must implement reasonable security measures to protect personal data, including encryption, access control, monitoring for unauthorized access, and data backups etc. These safeguards ensure the confidentiality, integrity, and availability of data, and must include provisions for detecting and addressing breaches and maintenance of logs. Contracts with Data Processors must also ensure security measures are in place. The measures should comply with technical and organizational standards to prevent data breaches.

7. Intimation of Personal Data Breach: When a Data Fiduciary becomes aware of a personal data breach, it is required to promptly notify all affected Data Principals. This notification must be clear and straightforward, explaining the breach's nature, extent, and timing, along with potential consequences for the affected individuals. The Data Fiduciary must also inform the Data Principal of any measures taken to mitigate the risks and provide safety recommendations for protecting their data. Furthermore, contact information of a responsible person for inquiries must be included.

Additionally, the Data Fiduciary must inform the Board about the breach without delay. Within 72 hours or a longer time if permitted, the Data Fiduciary is obligated to provide detailed information, including the events that led to the breach, actions taken to mitigate risks, and the identity of the individual responsible, if known. The Data Fiduciary must also report on the remedial steps taken to prevent future breaches and details on the notifications sent to affected Data Principals.

8. Time period for specified purpose to be deemed as no longer being served: Under this provision, if a Data Fiduciary processes personal data for purposes outlined in Schedule III and the Data Principal does not engage with the Fiduciary within a specified period, the personal data must be erased unless required for legal compliance. The time period for this erasure is defined in Schedule III for different classes of Data Fiduciaries, such as e-commerce entities, online gaming intermediaries, and social media

platforms. These entities may retain personal data for up to three years from the last interaction or the coming in effect of rules, whichever is later, except when the data is needed for the principal to access their account or virtual tokens.

Before erasure, the Data Fiduciary must notify the Data Principal at least 48 hours in advance, alerting them that their data will be erased unless they log in or initiate contact with the Fiduciary to fulfil the specified purpose. The notification gives the Data Principal an opportunity to preserve their data by taking action. This rule provides a clear process for erasing personal data if the Data Principal has not interacted with the Data Fiduciary within the specified time, ensuring that data is retained only when necessary for continued use or legal obligations, while offering the Data Principal a chance to retain their data by taking proactive steps.

9. Contact information for addressing data processing queries: This mandates that every Data Fiduciary must clearly display on their website or app the contact details of a designated person who can address questions regarding the processing of personal data. If applicable, this could be the Data Protection Officer (DPO). The contact information should be easily accessible and visible to Data Principals, enable that they can reach out with any concerns or queries about how their personal data is being processed. Additionally, the same contact details must be included in all responses to communications from Data Principals who wish to exercise their rights under the Data Protection Act.

The intent of this provision is to ensure transparency and accountability in data processing practices of Data Fiduciaries, by providing clear contact information, easier access to Data Principals to inquire about their personal data and its processing.

10. Verifiable consent for processing personal data of children and persons with disabilities: This provision outlines the requirements for obtaining verifiable consent from parents or legal guardians before processing the personal data of children or persons with disabilities. Specifically, a Data Fiduciary must implement measures to ensure that the person providing consent for a child's data processing is the child's parent or legal guardian, and that the parent or guardian is identifiable. For a child, the Data Fiduciary must verify that the parent is an adult by using reliable identity details or a virtual token mapped to such details. This verification process is critical to ensure that consent is being given by a responsible adult, in compliance with relevant laws. Examples are provided to clarify how this process should work, particularly in cases where the parent is already a registered user or when the parent needs to provide identity details using a Digital Locker service.

11. Exemptions from obligations in processing personal data of children: This provision outlines certain exemptions to the standard requirements for processing the personal data of children, as stated in section 9 of the Act. These exemptions are applicable to specific types of Data Fiduciaries and for certain purposes, subject to conditions laid out in Schedule IV. According to Part A of the schedule, certain classes of Data Fiduciaries, such as healthcare professionals, educational institutions, and childcare providers, are exempt from specific provisions related to children's data. The processing of children's personal data by these entities is permitted, but it is restricted to specific activities like health services, educational activities, safety monitoring, and transportation tracking. These activities must be necessary for the well-being and safety of the child, ensuring that data processing is done within a defined and limited scope.

Disclaimer: The purpose of this explanatory note is only to make it easier to understand the provisions of the Rules. However, this explanatory note is not intended to form part of the Rules and shall not be considered for legal interpretation of any provision of the Rules.

Part B of the schedule outlines specific purposes for which the exemptions apply, such as processing for legal duties, issuing subsidies or benefits to children, creating user accounts for communication purposes, or ensuring the child does not have access to harmful information. In these cases, processing is restricted to what is necessary to perform the function, service, or duty, with an emphasis on protecting the child's best interests. The provision acknowledges that certain activities, such as verifying the age of a data subject to confirm they are not a child, also fall under this exemption, as long as the processing remains limited to the necessary scope. These exemptions aim to strike a balance between protecting children's personal data and enabling necessary activities for their health, education, and safety.

12. Additional obligations of Significant Data Fiduciaries: This provision brings specific responsibilities for Significant Data Fiduciaries. It mandates that these Fiduciaries must conduct a Data Protection Impact Assessment (DPIA) and a comprehensive audit once every year. The results of these assessments and audits must be reported to the Board, which need to contain key findings related to their adherence to data protection requirements.

Further, the provision holds Significant Data Fiduciaries accountable for verifying that any algorithmic software they use to process personal data does not pose a risk to the rights of Data Principals. This includes algorithms used for data hosting, storage, and sharing.

Entities must adopt measures to ensure that personal data identified by the Central Government is processed in compliance with specific restrictions, ensuring that the data and any related traffic data are not transferred outside of India.

13. Rights of Data Principals: Data Fiduciaries and Consent Managers must clearly publish on their website or app the process by which Data Principals can exercise their rights under the Act, including identifying details like usernames to facilitate identification. Data Principals can request to access and erase their personal data by contacting the Data Fiduciary. A Data Fiduciary must also provide clear timelines for responding grievances, ensuring an effective process with the necessary technical and organizational safeguards. Data Principals may nominate one or more individuals to exercise their rights under the law, following the procedures set by the Data Fiduciary and applicable legal norms.

14. Processing of personal data outside India: Data Fiduciaries processing data within India or in connection with offering goods or services to Data Principals from outside India must comply with any requirements the Central Government sets in respect of making such personal data available to a foreign State or its entities. This is intended to ensure that personal data remains protected under the Act.

15. Exemption from Act for research, archiving, or statistical purposes: The Act does not apply to the processing of personal data carried out for research, archiving, or statistical purposes if it adheres to the specific standards outlined in Schedule II. This exemption ensures that necessary data processing for academic and policy research can occur while maintaining certain safeguards and standards to protect personal data.

16. Appointment of Chairperson and other Members: A Search-cum-Selection Committee shall be formed by the Central Government to recommend candidates for the position of Chairperson of the Data Protection Board. The committee will be led by the Cabinet Secretary , Secretary MeitY, Secretary DLA and include two subject matter experts.

Disclaimer: The purpose of this explanatory note is only to make it easier to understand the provisions of the Rules. However, this explanatory note is not intended to form part of the Rules and shall not be considered for legal interpretation of any provision of the Rules.

Similarly, the committee will also recommend candidates for the position of other Board Members, with the Ministry of Electronics and Information Technology Secretary overseeing the process.

After considering the recommended individuals' suitability, the Central Government will appoint the Chairperson or Members to the Board.

17: Salary, allowances, and other terms of service for Chairperson and Members: the Rule provides for Salary, allowances, and other service-related conditions for the Chairperson and Members of the Data Protection Board are provided. The Chairperson is entitled to a consolidated salary of ₹4,50,000 per month, while each Member receives ₹4,00,000 per month, with no provisions for housing or a car. A detail description of service conditions is provided for in this Schedule V.

18: Procedure for meetings of the Board and authentication of orders: the Rule outlines the procedure for the meetings of the Data Protection Board, including how they are convened, conducted, and how decisions are made. The Chairperson is responsible for setting the date, time, place, and agenda of the meetings, with the authority to delegate these duties. Meetings are chaired by the Chairperson, or in her absence, by another Member chosen by those present. A quorum for the meetings is one-third of the Board's membership, and decisions are made by majority vote, with the Chairperson having a casting vote in the event of a tie. If a Member has a conflict of interest in any matter being discussed, they are prohibited from participating or voting on that matter. In urgent situations, the Chairperson has the authority to take immediate action, which must then be ratified at the next Board meeting. Additionally, certain issues may be decided by circulating the item to Members for approval, and the Chairperson or any authorized individual can authenticate the Board's orders, directions, or instruments. Also, the Board is required to complete inquiries within six months, extendable for a further three months if necessary.

19: Functioning of the Board as a digital office: The Board is to operate as a digital office, utilizing technology to conduct its proceedings efficiently. This provision allows the Board to adopt techno-legal measures to carry out its functions without requiring the physical presence of individuals. The Board retains the power to summon individuals and examine them under oath. The aim is to streamline processes, reduce the need for physical attendance, and enhance the overall efficiency of the Board's operations.

20: Terms and conditions of appointment and service of officers and employees of the Board: the rule outlines the procedures for the appointment and service terms of officers and employees working for the Data Protection Board. It specifies that the Board can appoint officers and employees necessary for carrying out its functions, with prior approval from the Central Government. The appointments can be made on deputation from various government bodies or public sector enterprises. Additionally, the officers and employees can be appointed from the National Institute for Smart Government, with salaries aligned to market standards and other terms decided by the Board.

Schedule VI elaborates on the specifics of the terms and conditions of service for these officers and employees.

21: Appeal to Appellate Tribunal: the rule outlines the process for filing appeals to the Appellate Tribunal for persons dissatisfied with orders or directions of the Board. The appeal must be submitted digitally, in line with the procedure set by the Appellate Tribunal on its website. The appeal is required to be accompanied by a fee, the Appellate Tribunal's Chairperson may decide to reduce or waive it.

Disclaimer: The purpose of this explanatory note is only to make it easier to understand the provisions of the Rules. However, this explanatory note is not intended to form part of the Rules and shall not be considered for legal interpretation of any provision of the Rules.

The Appellate Tribunal has the authority to regulate its procedures. Additionally, the Tribunal operates as a digital office, utilizing technology to conduct its proceedings, which eliminates the need for physical presence while retaining the power to summon individuals and administer oaths when necessary. This digital approach allows for more flexible and efficient handling of appeals.

22: Calling for information from Data Fiduciary or Intermediary: enables the Central Government to require Data Fiduciaries or intermediaries to provide specific information for purposes outlined in Schedule VII. In cases where the disclosure of information might compromise the sovereignty, integrity, or security of India, the authorized person may restrict disclosure unless prior written permission is obtained. Fulfilling these information requests is part of the legal obligations under Section 36 of the Act. The government is empowered to request data for various purposes, including national security, legal compliance, or to assess the status of certain Data Fiduciaries.

***

Disclaimer: The purpose of this explanatory note is only to make it easier to understand the provisions of the Rules. However, this explanatory note is not intended to form part of the Rules and shall not be considered for legal interpretation of any provision of the Rules.