Luthra and Luthra
LAW OFFICES INDIA

January 7th, 2025

UPDATE ON THE DIGITAL PERSONAL DATA PROTECTION RULES 2025

INTRODUCTION

On January 3, 2025, the Ministry of Electronics and Information Technology **("MeitY")** introduced the draft rules under the Digital Personal Data Protection **("DPDP")** Act 2023 **("DPDP Rules 2025")** for public consultation. The Government is seeking feedback on the DPDP Rules 2025 through the 'MyGov portal' till February 18, 2025.

The DPDP Rules 2025 are designed to elucidate upon the operational aspects under the DPDP Act 2023 to protect digital personal data. They provide a clear operational framework that translates the legislative intent of the DPDP Act 2023 into actionable guidelines. This clarity aids organizations in understanding their compliance obligations, thereby fostering a culture of accountability in data management practices.

The present note aims to highlight the key aspects of the DPDP Rules 2025 and discuss noteworthy obligations for companies from a data privacy compliance perspective. Certain ambiguous aspects that require further clarity from the MeitY are also highlighted.

ENFORCEMENT

Rule 1 of the DPDP Rules 2025 envisages a phased timeline for implementation. Provisions relating to the Data Protection Board **("DPB")** and Appellate Tribunal (Rules 16-20) will take effect immediately upon notification in the official gazette, while operational obligations prescribing rules about data fiduciaries and consent managers (Rules 3-15, 21, and 22) will be implemented later, on a specified date prescribed by the Central Government. This gradual implementation should provide businesses and companies with time for transition in order to align their operations even if clarity on specific timelines will be significant for effective preparation.

NOTICE REQUIREMENT

Rule 3 of the DPDP Rules 2025 provides that data fiduciaries are required to present notice in a **clear and understandable manner**, independent of any other information made available by the data fiduciary, so as to enable data principals to give **specific and informed consent** for processing of their personal data. Such notice should include **an itemized description of the personal data** sought to be processed; the **purpose of processing such data** and **an itemized description of the goods or services** to be provided or uses to be enabled by such processing. Further, such notice must also contain the **specific communication link** for the website/ application (or both) of the data fiduciary along with a description of any other available means through which the **data principal can withdraw her consent** (with the process being as simple

as the provision of original consent), exercise data principal rights and make a complaint to the DPB.

CONSENT MANAGERS

Rule 4 and the First Schedule to the DPDP Rules 2025 prescribes the eligibility and registration requirements, responsibilities, suspension and cancellation of registration requirements and compliance measures for Consent Managers. As per the DPDP Act 2023, Consent Managers are persons registered with the DPB who act as a single point of contact to enable data principals to give, manage, review, and withdraw their consent through a transparent and interoperable platform, for processing their personal data by data fiduciaries. The conditions for registration as a Consent Manager include incorporation of a company in India, adequacy of capital, minimum net worth requirements, earning capacity, independent certification regarding the conformity of its platform to data protection standards as may be published by the DPB, etc.

Such entities must ensure data security and maintain records of consents given, denied, or withdrawn. They must provide data principals with access to their consent records and facilitate data sharing in a secure manner. To become a Consent Manager, companies must register with the DPB and meet certain conditions along with ensuring adherence to obligations mentioned in the First Schedule of the DPDP Rules 2025. Further, such Consent Managers must operate in an independent capacity and avoid any conflicting interests with data fiduciaries so as to ensure seamless interaction and compliance.

Further, the foremost obligation of Consent Manager is to enable a Data Principal using its platform to give consent to the processing of her personal data **by a Data Fiduciary onboarded onto such platform**. In respect of such onboarding, there is no guidance under the DPDP Rules 2025 on the procedure to be adopted by Consent Managers to undertake such onboarding of the data fiduciaries.

NOTIFICATION OF PERSONAL DATA BREACH

The DPDP Act 2023 provides that in the event of a personal data breach, the data fiduciary shall give the DPB **and each affected data principal**, intimation of such breach in such form and manner as may be prescribed.

Rule 7 of the DPDP Rules 2025 clarify the timeline and procedure for notifying a personal data breach to both data principals and the DPB as prescribed in the DPDP Act 2023. Rule 7(1) and Rule 7(1)(a) mandate data fiduciaries to **report the data breach to the data principal** through their user account or any other mode of communication opted by the data principal, and to the DPB immediately **without any delay** with mandatory details such as a description of the breach **including its nature, extent, timing, location of occurrence; likely impact; probable safety measures to be taken, etc**., while Rule 7(2)(b) mandates data fiduciaries to provide a detailed

report on the data breach to the DPB within 72 hours (or within such extended timeline as permitted by the DPB on a request made in writing) with updated information including measures implemented or proposed to mitigate risk, findings of the investigation and remedial measures undertaken and intimations given to affected data principals.

In addition to reporting an incident to the DPB, the data fiduciaries may have to report the incident to Indian Computer Emergency Response Team (CERT-IN), sectoral regulators such as Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI) and Reserve Bank of India (RBI) (if required), and other appropriate bodies within different timelines.

Unlike the General Data Protection Regulation 2016 **("GDPR")** which requires the communication of personal data breach to data subject only when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the DPDP Act 2023 read with DPDP Rules 2025 requires communication of any data breach to affected data principals which would significantly increase compliance burden of businesses. In addition, while there may be subjectivity in relation to timelines involving the phrase "without delay", this works well as a broad guiding principle. Likewise, allowing flexibility in the timelines for submitting detailed data breach reports - by the phrase 'or within such extended timeline as permitted by the DPB on a request made in writing' (as outlined in Rule 7(2)(b)) is certainly positive. Laying down certain broad criteria for granting extensions by the DPB would help to maintain transparency and consistency.

DATA RETENTION AND ERASURE

Certain notified categories of data fiduciaries such as **social media intermediaries with over 20 million registered Indian users, e-commerce entities with over 20 million registered Indian users** and **online gaming platforms with more than five million Indian users** are required to delete personal data when the specified purpose is no longer being fulfilled. This occurs when the data principal does not approach the data fiduciary for the specified purpose or exercise its rights related to the data processing. **These data fiduciaries may retain personal data for up to three years from the last interaction with the data principal or from the implementation of the DPDP Rules 2025, whichever comes later,** unless the data is needed for the data principal to access their user account or redeem virtual tokens for money, goods, or services. Prior to deleting the data, the data fiduciary must notify the data principal at least 48 hours in advance and provide an opportunity for re-engagement to prevent the erasure.

Data fiduciaries not covered by the above thresholds (including those in social media, e-commerce and online gaming) will need to make individual decisions of when data can be considered to not serve the specified purpose and accordingly implement a retention timeline. In view of this carefully defining 'purpose' at the time of seeking consent and framing internal policies (back by commercial justifications regarding purpose time-framework) becomes crucial.

VERIFIABLE CONSENT

Rule 10 discusses the due diligence to be followed by data fiduciaries when obtaining verifiable consent from parents and lawful guardians to process the personal data of children and persons with disabilities, respectively. Moreover, Rule 10(1)(b) specifies that data fiduciaries can generate a virtual token to identify the parent of a child.

To this end, the DPDP Rules 2025 specify that in order to obtain parental consent, data fiduciaries must establish **reliable systems for verifying parents or guardians, though they have the flexibility to choose the method between using (i) existing information that the data fiduciary may have with itself about the parent (such as in cases where the parent is already registered on the platform of the data fiduciary) or in other cases (ii) to use government-authorized digital tokens or (iii) to use the voluntarily provided details available using the services of a Digital Locker.** Additionally, certain class of data fiduciaries such as clinical and mental health establishments, healthcare professionals, allied healthcare professionals, educational institutions, individual childcare providers and transportation service providers engaged by such persons are exempt from both the parental consent requirement and restrictions on tracking or behavioral monitoring of children, as long as their processing of personal data is limited to activities like healthcare, education, ensuring safety, which are necessary for the well-being and safety of the child. However, this exemption is not blanket and is subject to specific conditions, hence businesses should consider a risk-based approach to age verification, tracking, and behavioral monitoring to prevent potential harm.

It should be noted that the DPDP Rules 2025 do not prescribe a single specific method for identification of a person who claims to be a parent but provides alternatives such as using trusted age and identity data government-issued tokens. The data fiduciary must ensure the identity of the adult is reliable and verifiable which could involve a combination of documents, virtual tokens, or identity data from official government services like Digital Locker or Aadhar.

SIGNIFICANT DATA FIDUCIARIES ("SDFS")

Rule 12 of the DPDP Rules 2025 provides additional obligations for the SDFs, including conducting a annual data protection impact assessment and audit every twelve months. SDFs are also required to furnish a report to the DPB highlighting significant findings from the data protection impact assessment and audits. Rule 12(3) mandates due diligence on algorithmic software deployed to ensure that processing personal data does not pose risks to a data principal's rights while Rule 12(4) outlines potential data localization measures for significant data fiduciaries, specifying that certain types of personal data, as determined by a committee formed by the central government, would be restricted from being transferred outside the country.

It should be noted that the DPDP Rules 2025 have not identified who would be classified as a SDF to whom additional obligations would be applicable, however this may be notified subsequently. Further, the obligation for annual audits and Data Protection Impact Assessments may be onerous

to comply with. It is also unclear under the law on how SDFs should verify algorithmic software, hence it remains to be seen be seen how this requirement is translated into and implemented.

RIGHTS OF DATA PRINCIPAL

Data fiduciaries are required to publish on their website or app the details of the mechanisms through which data principals can exercise their rights including access to data and erasure using provided means and identifiers such as usernames or other identifiers like file numbers or customer/enrolment IDs, that may be needed to verify identity. Additionally, data fiduciaries must publish details of their grievance redressal system and provide clear timelines for responding to requests or grievances.

Data principals also have the right to access, erase, and nominate representatives for their personal data with data fiduciaries and Consent Managers required to offer transparent and accessible methods for exercising these rights.

REASONABLE SECURITY SAFEGUARDS

Data fiduciaries are required to adopt comprehensive technical and organizational measures to ensure continuous improvement in security practices. They must implement security measures such as encryption, obfuscation, virtual token mapping, and strict access controls. These safeguards must also be contractually reinforced between data fiduciaries and processors. To operationalize this requirement, existing contracts will need to be reviewed to clearly define the roles and responsibilities of both data fiduciaries and data principals. Further data fiduciaries must implement appropriate safeguard measures to control access to concerned computer resources and restrict unauthorized access to data along with maintaining visibility on data access through logging and real-time monitoring to detect and remediate unauthorized access.

CROSS-BORDER TRANSFER OF PERSONAL DATA

Rule 14 of the DPDP Rules 2025 specifies that the Government may prescribe specific requirements to data fiduciaries, which they must follow before sharing or transferring personal data (either processed within India or outside) with foreign governments or their agencies or entities.

Under the DPDP Act 2023, free transfer of personal data to any country or territory outside of India is permitted, except for those specifically restricted by the Government through a notification. However, the DPDP Rules 2025 seem to introduce new limitations on the transfer of personal data abroad. For SDF's, as already discussed above, the Government, following recommendations from a committee it establishes, may identify specific personal data sets and

traffic data that cannot be transferred outside India. This implies that SDFs could face data localization requirements for certain customer or user data.

The Government may also impose requirements (via a general or special order) for data fiduciaries to disclose personal data to foreign states or entities under the control of such states. The intent of this appears to be aimed at ensuring that personal data originating in India remains protected under the DPDP Act 2023, potentially safeguarding it from foreign surveillance. Multinational organizations will need to assess how these localization requirements when implemented, affect their operations and their ability to ensure compliance with foreign laws that mandate their Government's access to data managed by these entities in relation to their Indian operations.

It should be noted that the Government can invoke Rule 14 of the DPDP Rules 2025 if it determines that a foreign agency's data request threatens India's national security, public order, individual privacy rights protected by Indian law, or conflicts with India's diplomatic or strategic interests. The main purpose of Rule 14 appears to be to regulate how foreign agencies can access personal data related to India. It aims to establish effective oversight mechanism, checks, and balances before such data is accessed, stressing the need for the Indian government's approval when a foreign agency justifies its request on national security grounds.

EXEMPTION FOR RESEARCH, ARCHIVING AND STATISTICAL PURPOSES

Rule 15 delineates the standards to be followed as specified under the Second Schedule to the DPDP Rules 2025 while availing exemptions from the DPDP Act 2023 for research, archiving and statistical purposes. Processing of personal data for research, archiving or statistical purposes is exempt, subject to adherence to standards, implementation of appropriate technical and organizational measures to ensure effective observance of standards including lawful processing, data accuracy, data minimization, restricting retention until fulfilment of purpose, implementation of reasonable security safeguards to prevent personal data breaches, accountability of data fiduciaries for processing in accordance with the standards that ensure data is used lawfully, without making individual-specific decisions and maintaining responsible data governance practices.

GOVERNMENT REQUESTS

Government has wide powers to call for information whereby data fiduciaries or intermediaries may be required by the Government to provide information for purposes such as national security, legal compliance, or to assess their eligibility as SDF. Additionally, the relevant authorities must set a timeline for submitting such information. If disclosing the information could impact India's sovereignty, integrity, or security, the authorities may restrict data fiduciaries from revealing such requests for information.

This legal update is only for general informational purposes, and nothing in this update could possibly constitute legal advice (which can only be given after being formally engaged and familiarizing ourselves with all the relevant facts). However, should you have any queries, require any assistance, or clarifications, please feel free to contact at the below mentioned coordinates.

© Luthra and Luthra Law Offices India 2024. All rights reserved.

KEY CONTACTS

AVISHA GUPTA
Partner
Email - avishag@luthra.com

SOMYA YADAV
Senior Associate
Email - syadav@luthra.com

EISHANI PATNAIK
Associate
Email - epatnaik@luthra.com

OFFICES

NEW DELHI
1st and 9th Floors, Ashoka Estate,
24 Barakhamba Road, New Delhi - 110 001
T: +91 11 4121 5100 F: +91 11 2372 3909
E: delhi@luthra.com

MUMBAI
20th Floor, Indiabulls Finance Center,
Tower 2 Unit A2, Elphinstone Road,
Senapati Bapat Marg, Mumbai - 400 013
T: +91 22 4354 7000 ,
F: +91 22 6630 3700
E: mumbai@luthra.com

BENGALURU
3rd Floor, Onyx Centre, No. 5, Museum Road,
Bengaluru - 560 001
T: +91 80 4112 2800 / +91 80 4165 9245
F: +91 80 4112 2332
E: bengaluru@luthra.com

HYDERABAD
Serene Towers,
House No. 8-2-623/A,
Road No. 10, Banjara Hills,
Hyderabad, Telangana - 500034
T: +91 40 7969 6162
E: hyderabad@luthra.com

CHENNAI
Prestige Palladium Bayan,
8th Floor, Greams Road, Nungambakkam Division,
Egmore, Chennai - 600 006,
Tamil Nadu
T: +91 95604 88155
E: chennai@luthra.com